丢番图方程引论

曹珍富 著

哈尔滨工业大学出版社

内 容 提 要

丢番图方程(Diophantine equations)是数论的一个重要分支，国内外很多著名数学家都从事过它的研究。其中尤以 Roth、Baker和Faltings等人的工作最为突出(他们分别获得了国际数学家大会的Fields奖)。本书力求全面详细地介绍这一数学分支的研究成果和创造的方法(有些方法产生了新的数学分支)。

本书共分十章，分别为：引言、解丢番图方程的初等方法、解丢番图方程的高等方法、一次丢番图方程、二次丢番图方程、三次丢番图方程、四次丢番图方程、高次丢番图方程、指数丢番图方程和单位分数问题。其中有一些是作者本人的研究成果。

本书可供从事这一数学分支或相关学科(组合论、群论和编码理论等)的数学工作者、研究生以及有兴趣的大学生和中学生阅读、学习和参考。

丢 番 图 方 程 引 论

曹 珍 富 著

*

哈尔滨工业大学出版社出版

新华书店首都发行所发行

哈尔滨建工学院印刷厂印刷

*

开本787×1092 1/32 印张14.375 数字318 000

1989年3月第1版 1989年3月第1次印刷

印数1—700

ISBN 7-5603-0131-2/O·20 定价7.95元

序

数论是数学中的一个重要分支。古今中外许多著名数学家都曾从事过数论的研究。数论往往以它的问题简明易懂吸引了大批青年人和业余数学爱好者。然而，如果不脚踏实地的不断加强数学素养、扩展数学知识面，也是难以取得成功的。

本书作者曹珍富就是哈尔滨工业大学八年前的一位被数论所深深吸引的非数学专业的学生，后来逐渐走上了科学研究的道路，发表了不少论文，成为我国最年轻的一批数学副教授中的一员。这本书是他几年来对数论中的丢番图方程（即不定方程）这一分支学习、研究的一个总结，也是继1969年Mordell的《丢番图方程》一书问世后的又一部著作。

全书共分十章。除引言外，以二、三两章分别详细介绍解丢番图方程的初等方法和高等方法，这里把借助相应方法所得到的近期成果纳入习题的做法，将有助于增强读者研究问题的能力和信心。四到十章，则依次讲述从一次、二次、三次、四次直至高次的丢番图方程以及指数丢番图方程和单位分数问题等不同类型的专题，侧重阐明结果与获得结果的所用方法，这便于读者了解和掌握。因之，本书具有一定特色。

由于丢番图方程的相当部分并不涉及更多的数学基础，加之本书由浅入深、循序渐进，读者只要具备一些初等数论知识即可读懂书中的绝大部分内容。可见该书就是对大学

生、乃至部分中学生也都是一种可供阅读、参考的读物。

个人对于丢番图方程完全是门外汉。我国著名数学家柯召教授对此有一系列重要贡献。这本书的作者也得益于孙琦教授的指教甚多。对一个正在成长的年青数学工作者所撰写的专门书籍难免有不成熟之处，甚至还会不少。相信我国数论界的前辈和同行必将继续给予帮助、鼓励和指点。

吴 从 炘

识于哈尔滨工业大学

1987年10月31日

目　　录

第一章 引　言

§1 数论的特点

在如今众多的数学分支中，有些即使你具备了一定的数学基础，要读懂它的基础知识也有一定的困难，甚至要理解它的符号的含义也办不到；而有些却不需要任何数学基础，只要你有耐心地往下读，便可读懂它的绝大部分内容。数论这门古老的数学分支，它的基本内容便是属于后者。数论的问题简明易懂，即使是公认的Fermat大定理和Goldbach猜想等问题也是如此。正因为这样，历史上几乎所有的数学家都从事过数论的研究，而且许多数学家都是因为数论问题的简明易懂，通过自学获得成功的。但事情往往是这样，越是简明易懂的问题，解决起来越困难。也正因为如此，不知道有多少业余数学爱好者迷上了数论，但最终却一事无成。

数论起初只研究整数的一些基本性质，后来从十七世纪到十九世纪，大数学家Fermat，Euler，Legendre，Gauss等人大大地发展了数论的内容，现在数学界最著名的难题——Fermat 大定理便是这个时期提出来的。

今天的数论已经发展了十多个数论分支，诸如代数数论、分析数论、丢番图方程、丢番图逼近和丢番图几何等，许多内容已经发展到相当深刻的程度，以致于搞不同分支的数论同行间也无法相互交流。可以举一个例子，你如果想读懂丢番图几何方面的研究论文，在不具有相当好的代数、

拓扑等基础时，即使你在其他某个数论分支中做出过很好的工作，但也几乎是不可能的。

§2　丢番图方程及其主要成就

这本书将专门研究数论的一个分支——丢番图方程的各种基本类型。什么叫丢番图方程呢？如所周知，Fermat 大定理是Fermat于1637年左右在古希腊数学家丢番图（Diophantus）所著《算术》一书的空白处写下的注释，用如今的语言叙述，就是：不定方程

$$x^n+y^n=z^n,\quad n>2$$

没有正整数解。这就明显告诉我们，Fermat 大定理是属于不定方程的。所谓不定方程，是指未知数的个数多于方程个数的方程（或方程组）。数论中的不定方程，通常对解的范围有一定的限制，例如解限制在有理数、整数等范围内。这种带限制的不定方程早在公元三世纪初古希腊数学家丢番图就研究过，人们为了与其他分支中的不定方程区别，也称数论中的不定方程为丢番图方程（Diophantine equations）。正如丢番图几何一样，它是代数几何中曲线上的"点"带限制的部分。

在丢番图方程中，各种形式的不定方程是无穷无尽的。但解决问题的方法，从古至今都是不同的问题用不同的方法，其中显示出了人类高度的智慧。人们自然要问，是否存在一个一般地解不定方程的方法？这个问题的特殊情形是属于D.Hilbert 第十问题的。1900年，D.Hilbert 提出了23个著名的数学问题，其中第10个是：

设 $f(x_1, \cdots, x_n)$ 是任给的具有整系数的多项式，那

么是否存在一个只有有限步运算的方法来判定丢番图方程 $f(x_1, \cdots, x_n)=0$ 是否有解？

这个问题的一般回答是否定的[1]。不妨设 $f(x_1,\cdots,x_n)$ 为不可约多项式，则在 $n\geqslant 3$ 时不存在一个只有有限步运算的方法来判定丢番图方程 $f(x_1, \cdots, x_n)=0$ 是否有解。而在 $n=2$ 时，A.Baker定出了丢番图方程 $f(x_1, x_2)=0$ 解的上界[2]，因而存在一个有限步运算的方法判定 $f(x_1, x_2)=0$ 是否有解。但是，A.Baker定出的上界往往太大，常常用最快的电子计算机也不能计算出方程的全部解来。因此，即使对于方程 $f(x_1, x_2)=0$，要求出全部解来也不容易。

但是，A.Baker的工作不失为丢番图方程的重要成就。包括A.Baker在内，还有K.F.Roth，R.Deligne和G.Faltings都在丢番图方程上作出过杰出的贡献。1955年K.F.Roth证明了一个著名的定理[3]：设 θ 是一个 $n\geqslant 2$ 次的代数数，则 $\forall \varepsilon>0$，适合

$$\left|\theta-\frac{x}{y}\right|<\frac{1}{y^{2+\varepsilon}}$$

的整数 x，$y>0$ 仅有有限组。这一定理导致了二元 $n\geqslant 3$ 次的不可约多项式方程解的个数有限。1973年，R.Deligne证明了关于有限域上不定方程 $f(x_1, \cdots, x_n)=0$ 解的个数的猜想，即著名的A.Weil猜想[4]。而G.Faltings在1983年证明了L.J.Mordell猜想，即有理数域里亏格 $\geqslant 2$ 的代数曲线上仅有有限个有理点[5]。由此可以导出Fermat方程 $x^n+y^n=z^n$，$(x, y)=1$ 在 $n\geqslant 4$ 时最多仅有有限组正整数解。1985年D.R.Heath—Brown利用G.Faltings定理证明了 $\lim\limits_{s\to\infty}\frac{N(s)}{s}=0$，这里 $N(s)$ 表 $n\leqslant s$ 使 $x^n+y^n=z^n\,(n>2)$ 有

正整数解的那些n的个数[6]。即对“几乎所有”的正整数$n>2$，方程 $x^n+y^n=z^n$ 均没有正整数解。

因为K．F．Roth，A．Baker，R．Deligne和G．Faltings的出色工作，他们分别于1958年、1970年、1978年和1986年获得了国际数学家大会的菲尔兹（Fields）奖。

§3 解丢番图方程的困难性

解丢番图方程由于没有一个一般的方法，因而它向人类的智慧提出了挑战。有一些看上去简单的方程，但解决起来却相当困难，例如求不定方程

$$1+x^2=2y^4 \tag{1}$$

的正整数解x，y问题，在很长时间内数学家们只知道它有两组解$(x, y)=(1, 1)$，$(239, 13)$，但要回答它是否存在另外的解却不容易。直到1942年 W．Ljunggren 在认真研究四次域的单位数后，用了大量的现代数论的成果才最终证明：方程（1）最多有两组正整数解[7]。后来，人们感到W．Ljunggren的证明复杂又不初等，且方法上的技巧又太特殊，故大数学家L．J．Mordell向全世界提出了一个公开性的问题[8]：是否能找到一个简单的或初等的证明？这个问题直到现在仍未解决。

对于不定方程

$$x^x y^y=z^z,\ x>1,\ y>1, \tag{2}$$

著名数学家P．Erdös曾经猜想它没有正整数解。1940年我国著名数学家柯召否定了这一猜想，证明了方程（2）有无穷多组解[9]：

$$x=2^{2^{n+1}(2^n-n-1)+2n}(2^n-1)^{2(2^n-1)},$$

$$y = 2^{2^{n+1}(2^n - n - 1)}(2^n - 1)^{2(2^n - 1)+2}$$

$$z = 2^{2^{n+1}(2^n - n - 1)+n+1}(2^n - 1)^{2(2^n - 1)+1}$$

其中 $n>1$。1959 年 W.H.Mills 发现柯召得到的解均满足 $4xy=z^2$的条件，从而证明了[10]：1)如果$4xy>z^2$，则方程(2)没有正整数解；2)如果 $4xy=z^2$，则柯召找到的解是(2)的全部正整数解。1984年，S.Uchiyama证明了：如果 $4xy<z^2$，则方程(2)最多只有有限组正整数解[11]。这提醒我们，很可能方程(2)的全部正整数解都已包含在柯召得到的解中。但是，要证明这件事或者找到另外的解都很困难。

对于$n!$和组合数$\binom{n}{m}=\frac{n!}{m!(n-m)!}$也曾有过一些猜想和问题。例如方程

$$\binom{n}{m} = y^k,\quad n>m>1,\quad k>2 \qquad (3)$$

没有正整数解。这是1939年P.Erdös提出的一个猜想，直到1984年，才由本书作者解决了k为偶数的情形[12]；而k为奇数时，除了在1951年由P.Erdös本人解决了 $m>3$(此时方程(3)无正整数解）外，目前只有一些零碎的结果。要彻底证明P.Erdös的这个猜想还有一定的困难。另一个问题是，方程

$$n!+1=x^2$$

仅有正整数解 $(n, x)=(4, 5)$，$(5, 11)$ 和$(7, 71)$ 吗？P.Erdös和R.Obláth曾经解决了方程$n!=x^p \pm y^p$，$(x,y)=1$且$p>2$，但对 $p=2$ 无能为力[8]。G.J.Simmons 还提出，方程$n!=(m-1)m(m+1)$ 仅有正整数解$(m, n)=(2, 3)$，$(3, 4)$，$(5, 5)$ 和$(9, 6)$吗？这个问题也没有得到解决。

通常，解一个丢番图方程很大程度上由人们的数学基础和研究经验决定的。这常常导致初学者望而生畏。但也有些

初学者不了解丢番图方程的内容，以为丢番图方程是从属于初等数论的，就是初等数论中的几个小玩艺儿。因此，许多初学者在不具备一定数学基础的同时，就不切实际地去试图证明Fermat大定理。

§4 丢番图方程的内容和求解原则

丢番图方程的内容异常丰富，它的分类基本上是由方程的形式决定的。例如，可分为一次方程、二次方程、三次方程、高次方程、指数方程和一些特殊的类型。很多基本类型都是历史遗留下来的。当然近代也提出了许多新的类型，这是由于许多学科的交叉渗透产生的。例如，在代数数论、组合论和群论等数学分支中都提出了一些丢番图方程问题。

就丢番图方程的研究目的而言，人们希望尽可能一般性地求解某个类型，以期在另外的许多场合得到更多、更好地应用。有些问题在整数环上解决了，人们还愿意把它放到代数整环上去研究；有些问题用高深方法解决了，人们还希望用较为初等的方法去解决。这些做法的目的，无非是想通过这些研究产生新的结构或新的技巧，而构成这种新结构或新技巧的往往可能是新数学分支的萌芽，也可能对科学技术产生某些特殊的应用。

丢番图方程的内容异常丰富，但又没有一个统一的处理方法，这就决定了研究丢番图方程的困难性。一般说来，我们只能给出丢番图方程的求解原则，即综合利用各种初等的、高深的方法，将丢番图方程转化为若干容易处理的或有熟知结果的方程。这就告诉我们，需要有相当熟练的初等和高深的数学基础，才能在丢番图方程研究中取得好的成果。但

是，这也不是绝对的，在初等证明中，具有熟练的初等数论基础同样会做出好的成果。

§5 本书的特点

本书我们假定读者具有初等数论的知识。在用到超出初等数论知识时，我们列出主要结果而不加证明。另外，书中的许多问题和结果在没有注明出处时，均是引自作者的一些未经发表的思想与方法，还有些部分是引自 Mordell 的书 Diophantine equations。书中所有字母在不做特别说明的情况下，均表示整数。

本书的特点是，详细论述了各种类型的丢番图方程的解及其研究的几乎全部成果。尤其还较系统地介绍了解丢番图方程的方法，其中大量的成果和方法是近几年才得到的。

本书在表达和结构上也作了探索。为了让读者掌握解丢番图方程的方法，我们在第二、三两章里，选择了一些典型的问题（这些问题中，有许多都是数学家们的研究结果，这在后面的专题研究中将有介绍），详细地给出了求解过程。在让读者领会了这些方法和技巧后，我们除了选择一些基本的习题外，还列出数学家们若干用相应方法得到的近期的研究结果作为习题。这样做的目的是，能够增强读者（尤其是自学者）研究问题的信心和能力。我们在写作时，为了让读者有一个自然的过渡，在讲述解丢番图方程的方法时，对问题（包括例题和习题）的出处将不加注明（只有少部分例外）。但凡是数学家们的研究结果，都将在后面各章的专题研究中给以介绍。从第四章开始，是各个专题的专门研究。在这方面，我们不可能给出每一个定理的详细证明（否则在篇幅上

是不允许的）。我们采取以介绍结果和取得该结果所使用的方法为主，给出少量技巧性强、方法使用上比较特殊且篇幅比较简短的证明为辅的写作方法。我们认为，这样做对读者没有什么损失，况且每章末，我们还列出了较为详细的参考文献，便于读者进一步钻研时查阅。

应该指出，虽然本书从收集资料到定稿(1987年10月)用了许多年的时间，但仍可能有不少重要的成果被遗漏。又由于作者受水平的限制，书中也可能有不少错误和某些疏忽。尤其是作者本人的许多论点，可能还不够成熟，敬请前辈和同行们批评指正！

最后，这本书的写作始终是在哈尔滨工业大学校领导和数学系领导的支持、关心下进行的，特别是校长杨士勤教授和系主任吴从炘教授对本书的写作和出版帮助甚大。多年来，作者的业师、四川大学数学系的孙琦教授也给了很多关心和帮助。在此作者向他们致以诚挚的感谢！

参 考 文 献

[1] Martin, D., Amer. Math. Monthly, 80 (1973), 233—269.

[2] Baker, A., Phi. Tran. Roy. Soc. Lon., A, 263(1967), 273—291.

[3] Cassels, J.W.S., An introduction to Diophantine Approximation, Camb. Univ. Press, 1957.

[4] Katz, N., Proc. of Symposia in Pure Math., 28 (1976), 275—305. (AMS).

[5] Faltings, G., Invent. Math., 73 (1983),

349—366.

[6] Heath-Brown, D.R., Bull. London Math. Soc., 17 (1985), 15—16.

[7] Ljunggren, W., Avh. Norske Vid. Akad. Oslo, I, 5 (1942), #5, 27pp.

[8] Guy, R.K., Unsolved Problems in Number Theory, D6, 25, Springer-Verlag, 1981.

[9] Ko, C. (柯召), J. Chinese Math. Soc., 2 (1940), 205—207.

[10] Mills, W.H., Report Inst. Theory of Numbers, Boulder, Colo.1959, 258—268.

[11] Uchiyama, S., Trudy Mat. Inst.Steklov., 163 (1984), 237—243.

[12] Cao, Z.F. (曹珍富), Proc. Amer. Math. Soc., 98 (1986), 11—16.

第二章　解丢番图方程的初等方法

本章我们将介绍解丢番图方程的常用初等方法，包括简单同余法、分解因子法、无穷递降法、比较素数幂法、二次剩余法、Pell方程法和递推序列法等。这为以后各章的专题研究奠定了必备的基础。

§1　简单同余法

所谓简单同余法，是指对丢番图方程取某个正整数$M>1$为模来制造矛盾的方法。这种方法的要点是根据所给方程的特点，选择模M。现举例说明。

1. 选择模$2^a(a>1)$。例如方程

$$x_1^2+x_2^2=4x_3+3 \qquad (1)$$

没有整数解。可以取模4：由于$x_1^2\equiv 0, 1 \pmod 4$，$x_2^2\equiv 0, 1 \pmod 4$，故$x_1^2+x_2^2\equiv 0, 1, 2 \pmod 4$。而方程(1)给出$x_1^2+x_2^2\equiv 3 \pmod 4$，这是矛盾的。

利用方程(1)，可以推出，方程

$$x_1^2+x_2^2=(4a+3)x_3^2 \qquad (2)$$

仅有整数解$x_1=x_2=x_3=0$。这是因为，除去$x_1=x_2=x_3=0$外，可以假设$(x_1, x_2, x_3)=1$。由(1)知$x_3\not\equiv 1 \pmod 2$，即$x_3\equiv 0 \pmod 2$，由(2)推出x_1，x_2同奇同偶。但$(x_1, x_2, x_3)=1$，故x_1，x_2只能是同奇。所以$x_1^2\equiv x_2^2\equiv 1 \pmod 4$，

(2) 给出 $2\equiv x_1^2+x_2^2=(4a+3)x_3^2\equiv 0 \pmod 4$，这不可能。

同样道理，对如下的丢番图方程取模8知，均无整数解：

$$x_1^2+2x_2^2=8x_3+5 \quad \text{或} 8x_3+7, \tag{3}$$

$$x_1^2-2x_2^2=8x_3+3 \quad \text{或} 8x_3+5, \tag{4}$$

和

$$x_1^2+x_2^2+x_3^2=4^a(8x_4+7)。 \tag{5}$$

例如对方程（3），（4），由于对任一数 x，均有 $x^2\equiv 0$，1，$4 \pmod 8$，故 $x_1^2+2x_2^2\not\equiv 5$，7 $\pmod 8$，$x_1^2-2x_2^2\not\equiv 3$，5 $\pmod 8$，即(3)和(4)均无整数解。对方程(5)显然 $a\geqslant 0$。如果$a\geqslant 1$，则对(5)取模4知 $x_1\equiv x_2\equiv x_3\equiv 0 \pmod 2$。于是可在(5)两端除去因子4。这样不失一般可设 $a=0$，但 $x_1^2+x_2^2+x_3^2\not\equiv 7 \pmod 8$，因此(5)无整数解。

利用$2^a(a>1)$为模解不定方程，主要利用以下的一些事实：

1） 对任意整数x，有$x^2\equiv 0$，$1 \pmod 4$；如x为奇数，则$x^2\equiv 1 \pmod 8$；

2） 设$k\geqslant 4$时，对任意的x，有$x^{2^{k-2}}\equiv 0$，$1 \pmod{2^k}$。

2． 选择模$3^a(a\geqslant 1)$。例如方程

$$(3a+1)x_1^2+(3b+1)x_2^2=3x_3^2 \tag{6}$$

仅有整数解$x_1=x_2=x_3=0$。因为除去$x_1=x_2=x_3=0$的解外，可设 $(x_1, x_2, x_3)=1$。于是取模3得 $x_1^2+x_2^2\equiv 0 \pmod 3$，而$x_1^2\equiv 0$，$1 \pmod 3$，故推出$x_1\equiv x_2\equiv 0 \pmod 3$，由(6)推出$x_3\equiv 0 \pmod 3$，与$(x_1, x_2, x_3)=1$矛盾。

对于三次的丢番图方程，常常需要取模 9 。例如如下的方程

$$x_1^3+x_2^3+x_3^3=9x_4\pm 4 \tag{7}$$

和

$$x_1^3+2x_2^3+4x_3^3=9x_4^3,\qquad x_1x_2x_3x_4\neq 0 \tag{8}$$

均无整数解。因为对任意整数x，有$x^3\equiv 0$，$\pm 1 \pmod 9$，所以对方程(7)有$x_1^3+x_2^3+x_3^3\not\equiv \pm 4 \pmod 9$，即(7)无解。而对方程(8)，除去$x_1=x_2=x_3=x_4=0$外，不失一般可设$(x_1, x_2, x_3, x_4)=1$。取模9知$x_1^3+2x_2^3+4x_3^3\equiv 0 \pmod 9$，故$x_1\equiv x_2\equiv x_3\equiv 0 \pmod 3$，由(8)推出$x_4\equiv 0 \pmod 3$，与$(x_1, x_2, x_3, x_4)=1$矛盾。

我们还可证方程

$$x_1^3+3x_1^2x_2+x_2^3=9x_3+2 \tag{9}$$

无整数解。这是因为对(9)取模3知$x_1+x_2\equiv 2 \pmod 3$，故有三种情形：1) $x_1\equiv x_2\equiv 1 \pmod 3$；2) $x_1\equiv 0 \pmod 3$，$x_2\equiv 2 \pmod 3$；3) $x_1\equiv 2 \pmod 3$，$x_2\equiv 0 \pmod 3$。在1)时$x_1^3\equiv x_2^3\equiv 1 \pmod 9$，故对(9)取模9得：$2+3x_1^2x_2\equiv 2 \pmod 9$，此推出$x_1^2x_2\equiv 0 \pmod 3$与$x_1\equiv x_2\equiv 1 \pmod 3$矛盾；在2)时$x_1^3\equiv 0 \pmod 9$，$x_2^3\equiv 8\equiv -1 \pmod 9$和$3x_1^2x_2\equiv 0 \pmod 9$，故(9)给出$-1\equiv 2 \pmod 9$，此也不可能；在3)时，与2)类似，(9)仍无整数解。

由(9)可知方程

$$x_1^3+3x_1^2x_2+x_2^3=9x_3-2 \tag{10}$$

也无整数解。这是因为(10)可化为

$$(-x_1)^3+3(-x_1)^2(-x_2)+(-x_2)^3=9(-x_3)+2。$$

利用方程(9)和(10)的结果可以推出，方程

$$x_1^3+3x_1^2x_2+x_2^3=(9a+2)x_3^3 \tag{11}$$

仅有整数解$x_1=x_2=x_3=0$。这个结果的证明不难，例如，除开$x_1=x_2=x_3=0$，对方程(11)可不失一般地设$(x_1, x_2, x_3)=1$。当$x_3\equiv 0 \pmod 3$时，方程(11)推出$x_1\equiv x_2\equiv 0 \pmod 3$，与$(x_1, x_2, x_3)=1$矛盾；而当$x_3\equiv \pm 1 \pmod 3$

时，(11)的右端$\equiv\pm 2(\bmod 9)$，故由(9)和(10)的结果知，(11)不可能。

有些三次丢番图方程还需要取模7，例如方程

$$x_1^3+2=7x_2 \tag{12}$$

没有整数解。这是因为$x_1^3\equiv 0$，$\pm 1(\bmod 7)$。利用(12)的结果，可以证明方程

$$x_1^3+2x_2^3=7(x_3^3+2x_4^3) \tag{13}$$

仅有整数解$x_1=x_2=x_3=x_4=0$。因为除$x_1=x_2=x_3=x_4=0$外，可设方程(13)的解满足$(x_1, x_2, x_3, x_4)=1$。如果$7\nmid x_2$，则$x_2^3\equiv\pm 1(\bmod 7)$，所以(13)推出$(\pm x_1)^3+2\equiv 0(\bmod 7)$，由(12)的结果知，这是不可能的。如果$7|x_2$，由(13)推出$7|x_1$，可设$x_1=7y_1$，$x_2=7y_2$代入(13)式得出

$$7^2(y_1^3+2y_2^3)=x_3^3+2x_4^3$$

由前类似可知，上式给出$7|x_4$，$7|x_3$，这与$(x_1, x_2, x_3, x_4)=1$矛盾。

3. 选择模p（p为奇素数）。这种模的选择，主要依据二次剩余、三次剩余和四次剩余的一些熟知结果。例如，设a无平方因子，且a含有$4k+3$形的素因子，则方程

$$x_1^2+x_2^2=ax_3^2 \tag{14}$$

仅有$x_1=x_2=x_3=0$的整数解。因为除$x_1=x_2=x_3=0$外，可设方程(14)的解满足$(x_1, x_2, x_3)=1$。又由a含有素因子$p\equiv 3(\bmod 4)$知，(14)给出

$$x_1^2\equiv -x_2^2(\bmod p)$$

由于$p|x_2$推出$p|x_1$，$p^2|ax_3^2$。又a无平方因子，故$p|x_3$，与$(x_1, x_2, x_3)=1$矛盾。故$p\nmid x_1x_2$，上式给出

$$1=\left(\frac{x_1^2}{p}\right)=\left(\frac{-x_2^2}{p}\right)=\left(\frac{-1}{p}\right)=-1,$$

这不可能。其中$\left(\frac{a}{p}\right)$表勒让德符号。

根据$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$，与上面类似地有方程

$$x_1^2-2x_2^2=a_1x_3^2,\ a_1\text{无平方因子}$$

和

$$x_1^2+2x_2^2=a_2x_3^2,\ a_2\text{无平方因子}$$

均仅有整数解$x_1=x_2=x_3=0$。其中a_1含有素因子$p\equiv\pm3\pmod 8$，a_2含有素因子$p\equiv5,7\pmod 8$。

对于三次、四次的丢番图方程，常常需要三次剩余和四次剩余的某些结果。我们知道，k次剩余符号$\left(\frac{n}{p}\right)_k$定义为：设$k>1$，$p-1=kq$，这里$p$是奇素数，则有$\left(\frac{n}{p}\right)_k=(n^q)_p$。这里$(a)_p$表示$a$模$p$的绝对最小剩余，即$(a)_p\in\left\{-\frac{p-1}{2},\cdots,-1,0,1,\cdots,\frac{p-1}{2}\right\}$。对于$k=3$，4时有以下几个常用的结果：

1） 设$p\equiv1\pmod 6$，则

$$\left(\frac{2}{p}\right)_3=1\Longleftrightarrow\text{存在整数}u,\ v\text{使得}p=u^2+27v^2。$$

2） 设$p\equiv1\pmod 8$，$p=a^2+b^2$，$4|a$，则

$$\left(\frac{2}{p}\right)_4=(-1)^{\frac{a}{4}}。$$

3） 设$p\equiv1\pmod 4$，则$\left(\frac{-1}{p}\right)_4=(-1)^{\frac{p-1}{4}}$。

利用1)～3)，我们来求解几个丢番图方程。

例 1 设p为奇素数，则方程

$$x_1^3=2x_2^3+px_3^3,\quad \left(\frac{2}{p}\right)_3\neq 1 \tag{15}$$

仅有$x_1=x_2=x_3=0$的整数解

证 除去$x_1=x_2=x_3=0$后，可设方程（15）的解满足$(x_1, x_2, x_3)=1$。于是(15)取模p得

$$x_1^3\equiv 2x_2^3 \pmod{p}。$$

显然，如$p|x_2$，则$p|x_1$，推出$p|x_3$，与$(x_1, x_2, x_3)=1$矛盾。所以$p\nmid x_1x_2$，上式给出

$$1=\left(\frac{x_1^3}{p}\right)_3=\left(\frac{2x_2^3}{p}\right)_3=\left(\frac{2}{p}\right)_3\neq 1$$

这不可能。

例 2 设奇素数$p=a^2+b^2$，且$a\equiv 4 \pmod 8$，则方程

$$x_1^4=2x_2^4+px_3^2,\quad x_1x_2x_3\neq 0 \tag{16}$$

没有整数解。

证 对（16）取模p得

$$x_1^4\equiv 2x_2^4 \pmod{p},$$

而由（16）可见，不妨设$p\nmid x_1x_2$，故上式给出

$$1=\left(\frac{x_1^4}{p}\right)_4=\left(\frac{2x_2^4}{p}\right)_4=\left(\frac{2}{p}\right)_4=(-1)^{\frac{a}{4}}=-1,$$

此不可能。

例 3 设素数$p\equiv 1 \pmod 8$，且$\left(\frac{2}{p}\right)_4\neq 1$，则方程

$$2x_1^2+1=px_2^2 \tag{17}$$

无整数解。

证 可设$x_1=2^s x_3$，$2\nmid x_3$，则对(17)式取模x_3得$1\equiv p x_2^2 \pmod{x_3}$，此即

$$1=\left(\frac{px_2^2}{x_3}\right)=\left(\frac{p}{x_3}\right)=\left(\frac{x_3}{p}\right),$$

所以

$$\left(\frac{x_1}{p}\right)=\left(\frac{2^s x_3}{p}\right)=\left(\frac{x_3}{p}\right)=1。$$

于是知，存在整数k使得$k^2\equiv x_1 \pmod p$，再对(17)取模p得

$$2k^4+1\equiv 0 \pmod p,$$

此给出

$$1=\left(\frac{-1}{p}\right)_4=\left(\frac{2k^4}{p}\right)_4=\left(\frac{2}{p}\right)_4\neq 1,$$

这证明了我们的结论。

还有一些题目，需要用到二次互反律。例如，证明方程

$$x_1^2+qx_2^2=p,\ p,\ q\text{是素数} \tag{18}$$

在$p\equiv 3 \pmod 4$，$q\equiv 1 \pmod 4$时无整数解。从(18)可知 $\left(\frac{p}{q}\right)=1$，$\left(\frac{-q}{p}\right)=1$，故有

$$1=\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=-\left(\frac{-q}{p}\right)=-1,$$

矛盾。

由上面地讨论可见，简单同余法可以用来否定丢番图方程无解，也可用来得出丢番图方程仅有零解。对于丢番图方程

$$f(x_1,\ \cdots,\ x_n)=0 \tag{19}$$

选择适当的模$M>1$，可以通过解同余式

$$f(x_1,\ \cdots,\ x_n)\equiv 0 \pmod M \tag{20}$$

来判断(19)是否有解。这是因为显然有如下的定理。

定理 如果丢番图方程(19)有整数解，则同余式(20)必有解。

我们也看到，这个定理的逆一般是不成立的。即同余式（20）有解，（19）不一定有整数解。例如，设 p，q 均是奇素数，$p \neq q$ 且 $\left(\frac{q}{p}\right)=1$，则同余式

$$x_1^2 - q x_2^2 \equiv 0 \pmod{p}$$

有解，但 $x_1^2 - q x_2^2 = 0$ 没有整数解。

习　　题

1. 设1）$a \equiv b \equiv c \equiv 1 \pmod{2}$ 和 $a \equiv b \equiv c \pmod{4}$ 或 2）$\frac{a}{2} \equiv b \equiv c \equiv 1 \pmod{2}$ 和 $b+c \equiv a$ 或 $4 \pmod{8}$，证明丢番图方程

$$a x_1^2 + b x_2^2 + c x_3^2 = 0,\quad abc \neq 0$$

仅有整数解 $x_1 = x_2 = x_3 = 0$。

2. 设 $a+b \equiv 0 \pmod{2}$，$cd \equiv 1 \pmod{4}$ 和 $k \equiv 1 \pmod{2}$，证明丢番图方程

$$(a x_1^2 + b x_2^2)^2 - 2k(c x_1^2 + d x_2^2)^2 = x_3^2$$

仅有整数解 $x_1 = x_2 = x_3 = 0$。

3. 证明丢番图方程 $15x_1^2 - 7x_2^2 = 9$ 无整数解。

4. 证明丢番图方程 $x_1^3 + 2x_2^3 + 4x_3^3 + x_1 x_2 x_3 = 0$，$x_1 x_2 x_3 \neq 0$ 无整数解。

5. 设素数 $p \equiv 1 \pmod{8}$ 且 $p = a^2 + b^2$，$a \equiv 4 \pmod{8}$，证明丢番图方程 $x_1^4 = p x_2^4 + 2x_3^2$ 仅有整数解 $x_1 = x_2 = x_3 = 0$。

6. 证明丢番图方程 $y^2 = x^3 + 7$ 以及 $y^2 = x^3 - 3$ 均无整数解。

7. 证明丢番图方程 $3^x + 4^y = 5^z$ 仅有正整数解 $x = y = z = 2$。

§2 分解因子法

分解因子法，是将所给的丢番图方程经过整理，化为

$$f(x_1, \cdots, x_m) = Dy^n, \ n>1 \qquad (1)$$

然后分解f为两项乘积形式，即$f = f_1 f_2$。则根据唯一分解定理，由(1)得到

$$f_1 = D_1 y_1^n, \qquad f_2 = D_2 y_2^n$$

其中$Dy^n = D_1 D_2 (y_1 y_2)^n$。这样可使问题得到简化。例如，著名的Catalan 方程

$$x^2 - 1 = y^n, \ n \geqslant 3, \ xy \neq 0 \qquad (2)$$

在$2 | x$时无整数解。这是因为(2)可化为$(x-1)(x+1) = y^n$，而在$2|x$时$(x-1, x+1) = 1$，故有

$$x - 1 = y_1^n, \ x + 1 = y_2^n, \ y = y_1 y_2,$$

此给出

$$2 = y_2^n - y_1^n = (y_2 - y_1)(y_2^{n-1} + \cdots + y_1^{n-1}) > 2,$$

故论断正确。现在我们举一些例子，以说明这种方法的用法。

例 1 丢番图方程

$$x^2 + y^2 = z^2, \ x>0, \ y>0, \ z>0 \qquad (3)$$

的全部整数解可表为（x，y可互换）

$$x = 2abd, \ y = (a^2 - b^2)d, \ z = (a^2 + b^2)d \qquad (4)$$

其中d是正整数，$a>b>0$，$(a, b) = 1$且a，b一奇一偶。

证 设$(x, y) = d$，则(3)给出$d|z$。故可令$x = dx_1$，$y = dy_1$，$z = dz_1$，这里x_1，y_1和z_1均是正整数。于是方程(3)化为

$$x_1^2 + y_1^2 = z_1^2, \ (x_1, y_1) = 1, x_1>0, y_1>0, z_1>0 \qquad (5)$$

由于x_1，y_1同奇由(5)推出$z_1^2 = x_1^2 + y_1^2 \equiv 2 \pmod 4$的矛

盾结果，故可设x_1，y_1一奇一偶，令x_1为偶，则由(5)化为

$$\left(\frac{x_1}{2}\right)^2=\frac{z_1^2-y_1^2}{4}=\left(\frac{z_1+y_1}{2}\right)\left(\frac{z_1-y_1}{2}\right), \quad (6)$$

由于$\left(\frac{z_1+y_1}{2}, \frac{z_1-y_1}{2}\right)=(z_1, y_1)=(y_1, x_1)=1$。故(6)给出

$$\frac{z_1+y_1}{2}=a^2, \quad \frac{z_1-y_1}{2}=b^2, \quad \frac{x_1}{2}=ab,$$

这里 $a>b>0$，$(a, b)=1$ 且 a，b 一奇一偶。由上式解出 $x_1=2ab$，$y_1=a^2-b^2$，$z_1=a^2+b^2$。这就证明由（3）可推出（4）。

反之，容易验算（4）满足（3）。证毕。

例 2 丢番图方程

$$x^4-2y^2=1 \quad (7)$$

仅有整数解$x=\pm1$，$y=0$。

证 由（7）显然$2\nmid x$，$2|y$。故（7）可整理成

$$\left(\frac{x^2-1}{2}\right)\left(\frac{x^2+1}{2}\right)=2\left(\frac{y}{2}\right)^2, \quad (8)$$

因为$\left(\frac{x^2-1}{2}, \frac{x^2+1}{2}\right)=1$ 且$\frac{x^2+1}{2}\equiv1 \pmod 2$，故（8）给出

$$\frac{x^2+1}{2}=y_1^2, \quad \frac{x^2-1}{2}=2y_2^2, \quad y=2y_1y_2,$$

这里$(y_1, y_2)=1$。由$\frac{x^2-1}{2}=2y_2^2$知$x^2-4y_2^2=1$，即有$x+2y_2=\pm1$，$x-2y_2=\pm1$，推出 $x=\pm1$，$y_2=0$。从而$y=2y_1y_2=0$。证毕。

例 3 设p是一个奇素数，则丢番图方程

$$4x^4 - py^2 = 1 \tag{9}$$

除开$p=3$，$x=y=1$和$p=7$，$x=2$，$y=3$ 外，无其他的正整数解。

证 所给方程化为

$$(2x^2-1)(2x^2+1)=py^2,$$

由于 $(2x^2-1,\ 2x^2+1)=1$，p是一个奇素数，故上式给出

$$2x^2 \pm 1 = py_1^2,\quad 2x^2 \mp 1 = y_2^2,\quad y = y_1 y_2 \tag{10}$$

其中 $(y_1,\ y_2)=1$。由（10）的前两式得

$$4x^2 = py_1^2 + y_2^2,$$

此式可整理成

$$(2x+y_2)(2x-y_2)=py_1^2 \tag{11}$$

由于 $(2x+y_2,\ 2x-y_2)=(x,\ y_2)=1$，故(11)式给出

$$2x \pm y_2 = py_3^2,\quad 2x \mp y_2 = y_4^2,\quad y_1 = y_3 y_4, \tag{12}$$

其中 $(y_3,\ y_4)=1$。由此解出 $x=\dfrac{py_3^2+y_4^2}{4}$，$y_1=y_3y_4$，代入（10）的第一式得

$$2\left(\frac{py_3^2+y_4^2}{4}\right)^2 \pm 1 = py_3^2 y_4^2,$$

由此整理得

$$y_4^4 - 2\left(\frac{py_3^2-3y_4^2}{4}\right)^2 = \pm 1。 \tag{13}$$

取"+"号时，由例2知（13)式给出 $y_4^2=1$，$\dfrac{py_3^2-3y_4^2}{4}=0$，即给出方程（9）的正整数解$p=3$，$x=y=1$；取"−"号时，(13)是方程$x^4+y^4=2z^2$，$(x,\ y)=1$ 的特殊情形，由§3的例 3 知，(13)给出$y_4^2=1$，$\dfrac{py_3^2-3y_4^2}{4}=\pm 1$，此给

出方程（9）的正整数解$p=7$，$x=2$，$y=3$。证毕。

例 4 丢番图方程

$$x^3-1=2y^2 \tag{14}$$

仅有整数解 $x=1$，$y=0$ 。

证 显然，若（14）有另外的解，可设 $x>1$，$y>0$ 。改写（14）为

$$(x-1)(x^2+x+1)=2y^2 \tag{15}$$

因为$(x-1,\ x^2+x+1)=1$或3 且由（14）知 $2\nmid x$，故(15)给出

$$x-1=2y_1^2, x^2+x+1=y_2^2, y=y_1y_2, y_1>0, y_2>0, \tag{16}$$

或

$$x-1=6y_1^2,\ x^2+x+1=3y_2^2,\ y=3y_1y_2,\ y_1>0,\ y_2>0, \tag{17}$$

其中$(y_1,y_2)=1$。由(16)的第二式得 $(2y_2)^2=(2x+1)^2+$ ，此即 $(2y_2-2x-1)(2y_2+2x+1)=3$，由此知道$y_2=1$，$x=0$，与$x>1$矛盾。

对于（17）式，将$x=6y_1^2+1$代入$x^2+x+1=3y_2^2$得

$$(2y_2)^2-1=3(4y_1^2+1)^2,$$

此式可整理成

$$(2y_2-1)(2y_2+1)=3(4y_1^2+1)^2,$$

故得出

$$2y_2-1=3y_3^2, 2y_2+1=y_4^2, 4y_1^2+1=y_3y_4,\ y_3>0, y_4>0, \tag{18}$$

或

$$2y_2-1=y_3^2, 2y_2+1=3y_4^2, 4y_1^2+1=y_3y_4,\ y_3>0, y_4>0, \tag{19}$$

其中$(y_3,\ y_4)=1$ 。对于（18），由 $4y_1^2+1=y_3y_4$ 知 $2\nmid$

y_3y_4，故由$2y_2-1=3y_3^2\equiv3\pmod 8$知$2y_2\equiv4\pmod 8$；但由$2y_2+1=y_4^2\equiv1\pmod 8$知$2y_2\equiv0\pmod 8$。故(18)不可能。

现在来证明（19）也不可能。由（19）的前两式得$y_3^2-3y_4^2=-2$，故由$4y_1^2+1=y_3y_4$得出

$$8y_1^2=2y_3y_4-2=2y_3y_4+y_3^2-3y_4^2$$
$$=(y_3-y_4)(y_3+3y_4),$$

因为从$4y_1^2+1=y_3y_4$知$y_3\equiv y_4\pmod 4$，故上式即为

$$2\left(\frac{y_1}{2}\right)^2=\left(\frac{y_3-y_4}{4}\right)\left(\frac{y_3+3y_4}{4}\right), \qquad (20)$$

而$\left(\frac{y_3-y_4}{4},\ \frac{y_3+3y_4}{4}\right)=(y_4,\ y_3)=1$，故（20）给出

$$\frac{y_3-y_4}{4}=2y_5^2,\quad \frac{y_3+3y_4}{4}=y_6^2,\quad y_5>0, y_6>0, \qquad (21)$$

或

$$\frac{y_3-y_4}{4}=y_5^2,\quad \frac{y_3+3y_4}{4}=2y_6^2,\quad y_5>0, y_6>0, \qquad (22)$$

其中$y_1=2y_5y_6$且$(y_5,\ y_6)=1$。由（21）解出$y_3=y_6^2+6y_5^2$，$y_4=y_6^2-2y_5^2$，代入$y_3^2-3y_4^2=-2$得

$$y_6^4-12y_5^2y_6^2-12y_5^4=1$$

由此整理成

$$4y_6^4-3(y_6^2+2y_5^2)^2=1,$$

此由例3知仅有$y_6^2=1$，$y_6^2+2y_5^2=1$，推出$y=0$，与假设$y>0$矛盾。

同理，由（22）解出$y_3=2y_6^2+3y_5^2$，$y_4=2y_6^2-y_5^2$，代入$y_3^2-3y_4^2=-2$得

$$4y_6^4-12y_6^2y_5^2-3y_5^4=1$$

由此整理得

$$16y_6^4-3(y_5^2+2y_6^2)^2=1,$$

但对此取模 8 知仍不可能。证毕。

分解因子法，是一种技巧性很强的初等方法，很多步骤上的想法都是跳跃性的。由于这种方法的实质，是把丢番图方程不断展开，化为容易处理或有熟知结果的方程，因此使用这种方法常常需要有这方面较为丰富的知识和经验。

最后，对于一般的丢番图方程

$$f(x_1,\ \cdots,\ x_s)=g(y_1,\ \cdots,\ y_t),\qquad(23)$$

如果 f 和 g 都可分解，令

$$f=f_1f_2,\quad g=g_1g_2,$$

则在 $g_1\neq0$ 时，可令 $f_1=\lambda g_1$，$\lambda=\frac{a}{b}$，$(a,\ b)=1$，代入 (23) 得 $g_2=\lambda f_2$，于是把 (23) 化为解方程组

$$bf_1=ag_1,\quad af_2=bg_2。$$

利用这种方法可以求出方程 (23) 的全部解，也可用来构造方程 (23) 的部分解。例如求方程

$$x^4+y^4+z^4=w^2\qquad(24)$$

的整数解。由

$$(XY)^4+(YZ)^4+(XZ)^4=W^2$$

整理得

$$Y^4(X^4+Z^4)=W^2-X^4Z^4=(W-X^2Z^2)(W+X^2Z^2),$$

令

$$W-X^2Z^2=\lambda Y^4,\quad W+X^2Z^2=\frac{1}{\lambda}(X^4+Z^4),$$

消去 W 得

$$X^4+Z^4-2\lambda X^2Z^2=\lambda^2Y^4$$

令 $\lambda=1$，上式给出 $(X^2-Z^2)^2=Y^4$，即 $X^2-Z^2=Y^2$（或$X^2-Z^2=-Y^2$），于是由例1知

$$X=(a^2+b^2)d,\quad Y=2abd,\quad Z=(a^2-b^2)d,$$

这样，我们可得出方程（24）的部分整数解如下：

$$x=XY=2ab(a^2+b^2)d^2,$$

$$y=YZ=2ab(a^2-b^2)d^2,$$

$$z=XZ=(a^4-b^4)d^2,$$

$$w=W=Y^4+X^2Z^2=(16a^4b^4+(a^4-b^4)^2)d^4。$$

下面我们给出用这种方法求出所给方程的全部解的例子。

例 5 丢番图方程

$$x_1^2+\cdots+x_n^2=x^2,\quad (x_1,\cdots,x_n)=1,n>1,x>0, \tag{25}$$

的全部整数解由下式给出：

$$dx_i=2X_iX_n\ (i=1,\ \cdots,\ n-1),$$

$$dx_n=X_n^2-X_1^2-\cdots-X_{n-1}^2,$$

$$dx=X_n^2+X_1^2+\cdots+X_{n-1}^2,$$

这里 $(X_1,\ \cdots,\ X_n)=1$，$d>0$使得 $(x_1,\ \cdots,\ x_n)=1$。

证 设

$$x_1=tX_1',\ \cdots,\ x_{n-1}=tX_{n-1}',$$

则（25）式给出

$$t^2(X_1'^2+\cdots+X_{n-1}'^2)=x^2-x_n^2=(x-x_n)(x+x_n)。$$

令$x+x_n=\lambda t$，$x-x_n=\frac{t}{\lambda}(X_1'^2+\cdots+X_{n-1}'^2)$，这里 $\lambda=\frac{X_n}{b}$，$(X_n,\ b)=1$。于是

$$b(x+x_n)=X_nt,\quad X_n(x-x_n)=bt(X_1'^2+\cdots+X_{n-1}'^2)。$$

由$b(x+x_n)=X_nt$知$b|t$，令 $t=bt_1$，则有

$$x_n=X_nt_1-x,\quad X_n(x-x_n)=b^2t_1(X_1'^2+\cdots+X_{n-1}'^2)。$$

令$X_i=bX_i'$（$i=1, \cdots, n-1$），则有

$$x_i=bt_1X_i'=t_1X_i\quad(i=1, \cdots, n-1),$$

$$t_1(X_1^2+\cdots+X_n^2)=2xX_n,$$

$$t_1(X_n^2-X_1^2-\cdots-X_{n-1}^2)=2x_nX_n,$$

所以

$$\frac{x_1}{2X_1X_n}=\cdots=\frac{x_{n-1}}{2X_{n-1}X_n}=\frac{x_n}{X_n^2-X_1^2-\cdots-X_{n-1}^2}$$

$$=\frac{x}{X_n^2+X_1^2+\cdots+X_{n-1}^2},$$

由此即得（25）的全部解公式，证毕。

这个例子的一个简单情形是$n=2$，即方程

$$x_1^2+x_2^2=x^2,\quad (x_1, x_2)=1$$

的全部解可表为

$$dx_1=2X_1X_2,\quad dx_2=X_2^2-X_1^2,\quad dx=X_2^2+X_1^2,$$

其中（X_1，X_2）$=1$。$d>0$ 使 （x_1，x_2）$=1$，故 $d=(2X_1X_2, X_2^2-X_1^2)=1$，这就给出例1的结果。

习　　题

1．求出丢番图方程$x^2+2y^2=z^2$和$x^2+y^2=2z^2$的全部整数解。

2．证明丢番图方程$x^3+1=2y^2$仅有正整数解 $x=y=1$和$x=23$，$y=78$。

3．证明丢番图方程$x^2-8y^4=1$ 仅有正整数解$x=3$，$y=1$。

4．设p是奇素数，则丢番图方程 $x^4-py^2=1$仅有正

整数解$p=5$，$x=3$，$y=4$和$p=29$，$x=99$，$y=1820$。

5. 证明丢番图方程$x^2-2y^4=1$ 没有正整数解。

6. 设$D>2$不是平方数，且D不被3或$6k+1$ 形素数整除，则如下丢番图方程均仅有 $y=0$ 的整数解：

$$x^3\pm1=Dy^2,$$
$$x^3\pm1=3Dy^2\text{。}$$

§3 无穷递降法

无穷递降法是费马创立的一种解丢番图方程的方法。设有方程

$$f(x_1,\ \cdots,\ x_n)=0,\ x_i>0\ (i=1,\ \cdots,\ n),\qquad(1)$$

无穷递降法是说，假定(1)有一组正整数解$x_1^{(0)},\cdots,x_n^{(0)}$，由(1) 可推出(1)必有正整数解$x_1^{(1)}$，…，$x_n^{(1)}$，且 $x_1^{(1)}<x_1^{(0)}$。由$x_1^{(1)}$，…，$x_n^{(1)}$是(1)的正整数解，又可推出$x_1^{(2)},\cdots,x_n^{(2)}$是(1)的正整数解，且$x_1^{(2)}<x_1^{(1)}$。这个手续可以一直做下去，得出(1)的无穷多组解，且有正的无穷递降序列

$$x_1^{(0)}>x_1^{(1)}>x_1^{(2)}>\cdots,$$

但这是不可能的，因为 $x_1^{(0)}$是有限的。这个矛盾是由我们假定(1)有一组正整数解造成的。

在实际使用无穷递降法时，常假设(1)的全体整数解中有一组使得 $x_1=x_1^{(1)}$ 为最小，推出(1)的另一组正整数解中$x_1=x_1^{(2)}<x_1^{(1)}$，从而导致矛盾。

例 1 丢番图方程

$$x^4+y^4=z^2\qquad(2)$$

仅有$xy=0$的整数解。

证 显然，方程(2) 除 $xy=0$ 外，不失一般设 $x>0$，

$y>0$，$z>0$，这里 $(x, y)=1$是(2) 的解中使z为最小的那组解。于是由§2的例1可知，(2)给出（不妨设$2|y$）

$$x^2=a^2-b^2,\quad y^2=2ab,\quad z=a^2+b^2,$$

其中$a>b>0$，$(a, b)=1$，且a，b一奇一偶。由于$x^2=a^2-b^2$，$2\nmid x$，所以$2\nmid a$，$2|b$。故由$x^2+b^2=a^2$可得

$$x=p^2-q^2,\quad b=2pq,\quad a=p^2+q^2,$$

其中$p>q>0$，$(p, q)=1$且p，q一奇一偶。于是

$$y^2=2ab=4pq(p^2+q^2),$$

由 $(p, q)=1$知，$(p, p^2+q^2)=(q, p^2+q^2)=1$，故上式给出

$p=r^2$，$q=s^2$，$p^2+q^2=z_1^2$，$r>0$，$s>0$，$z_1>0$，$(r,s)=1$，由此推出

$$r^4+s^4=z_1^2,\quad r>0,\quad s>0,\quad z_1>0,\quad (r, s)=1,$$

由于 $0<z_1=\sqrt{a}<z$，与z的假设矛盾。证毕。

利用例1很容易推出§2的例2，即丢番图方程

$$x^4-2y^2=1$$

仅有整数解$x=\pm1$，$y=0$。这是因为由$x^4-2y^2=1$ 可整理成

$$x^4+y^4=(y^2+1)^2。$$

例 2 丢番图方程

$$x^4-y^4=z^2,\quad (x, y)=1 \tag{3}$$

仅有整数解 $x^2=y^2=1$和$x^2=1$，$y=0$。

证 除 $x^2=y^2=1$ 和 $x^2=1$，$y=0$ 外，可设(3)有解$x>0$，$y>0$，$z>0$，且x是所有解中最小的。显然 $2\nmid x$ 且y是奇或偶。

如果$y\equiv1\pmod 2$，则由(3)得出

$x^2=a^2+b^2$，$y^2=a^2-b^2$，$z=2ab$，$(a, b)=1$，$a>b>0$，

从而

$$x^2y^2=a^4-b^4,\ (a,\ b)=1,$$

这是(3)的一个情形，但$0<a<x$，与x最小矛盾。

如果$y\equiv 0 \pmod 2$，则由(3)得出

$$x^2=a^2+b^2,\ y^2=2ab,\ (a,\ b)=1,\ a>0,\ b>0,$$

其中不妨设$a\equiv 0 \pmod 2$，$b\equiv 1 \pmod 2$。由$y^2=2ab$，$(a,\ b)=1$知

$$a=2p^2,\ b=q^2,\ (p,\ q)=1,\ p>0,\ q>0$$

代入 $x^2=a^2+b^2$ 得

$$x^2=4p^4+q^4,\ (p,\ q)=1,$$

由此知

$$p^2=rs,\ q^2=r^2-s^2,\ (r,\ s)=1,\ r>s>0,$$

但由$p^2=rs$，$(r,\ s)=1$ 推出 $r=u^2$，$s=v^2$，$(u,\ v)=1$，$u>0$，$v>0$，故

$$q^2=r^2-s^2=u^4-v^4,$$

但$0<u=\sqrt{r}\leqslant p<x$，仍与$x$为最小矛盾。证毕。

由这个证明过程可见，丢番图方程

$$4x^4+y^4=z^2,\ (x,\ y)=1 \qquad (4)$$

仅有整数解 $x^2=1$，$y=0$ 和 $x=0$，$y^2=1$。此外，由方程(3)的结果还可推出。

例 3 丢番图方程

$$x^4+y^4=2z^2,\ (x,\ y)=1 \qquad (5)$$

仅有整数解$x^2=y^2=1$。这是因为(5)式可整理成

$$z^4-x^4y^4=\left(\frac{x^4-y^4}{2}\right)^2。$$

例3的一个特殊情形是：方程$x^4-2y^2=-1$仅有整数解$x^2=y^2=1$。这个结果在研究其他一些丢番图方程问题时常常

用到。

无穷递降法在早期研究丢番图方程

$$x^4+kx^2y^2+y^4=z^2,\ (x,\ y)=1 \tag{6}$$

中起过重要作用。例1给出了方程(6)在$k=0$时的结果，利用例3我们还可以推出$k=6$的情形。

例 4 设$k=6$，则(6)仅有整数解$x^2=1, y=0$和$x=0$，$y^2=1$。

证 在$k=6$时，方程(6)即为

$$x^4+6x^2y^2+y^4=z^2,\ (x,\ y)=1 \tag{7}$$

设方程(7)有$x>0$，$y>0$的整数解，令

$$x+y=u,\quad x-y=v,$$

解出 $x=\frac{u+v}{2}$，$y=\frac{u-v}{2}$代入(7)，整理得

$$u^4+v^4=2z^2,$$

此由例3知 $u^2=v^2$，所以 $x=0$或$y=0$，证毕。

例 5 设 $k=-6$，则(6) 仅有整数解 $x^2=1$，$y=0$ 和 $x=0$，$y^2=1$。

证 在$k=-6$时方程(6)化为

$$x^4-6x^2y^2+y^4=z^2,\ (x,\ y)=1 \tag{8}$$

如果(8)存在另外的解，不妨设$x>y>0$。由方程(8)整理成

$$(x^2-y^2+z)(x^2-y^2-z)=4x^2y^2。 \tag{9}$$

我们来证明 $(x^2-y^2+z,\ z^2-y^2-z)=2$。首先，由$x^4-6x^2y^2+y^4=z^2$，$(x,\ y)=1$知 x，y 不能同奇，因不然有$x^4\equiv y^4\equiv 1 \pmod{16}$，$-6x^2y^2\equiv -6 \pmod{16}$，故$z^2=x^4-6x^2y^2+y^4\equiv -4 \pmod{16}$，这不可能。于是知$x$，$y$一奇一偶，因而 $z\equiv 1 \pmod 2$。设 $(x^2-y^2+z,\ x^2-y^2-z)=d$，显然$2|d$，$d|2z$。如果$d$有奇素数因子$p$，

则$p|d$，$p|z$。由$p|x^2-y^2+z$及(9)知$p|x^2-y^2$，$p|xy$，推出$p|x$，$p|y$，与$(x, y)=1$矛盾，于是$d=2$。由$x>y>0$知，(9)式给出

$$x^2-y^2+z=2a^2,\quad x^2-y^2-z=2b^2,\quad xy=ab,$$

其中$(a, b)=1$，$a>0$，$b>0$。由此可得

$$x^2-y^2=a^2+b^2,\quad xy=ab,$$

故

$$(x^2+y^2)^2=(x^2-y^2)^2+4x^2y^2=(a^2+b^2)^2+4a^2b^2$$
$$=a^4+6a^2b^2+b^4,$$

此由例 4 知不可能成立。证毕。

例3～例5都是例2的推论。

最后，我们用无穷递降法解决方程(6)当$k=\pm1$时的情形。

例 6 丢番图方程

$$x^4+x^2y^2+y^4=z^2,\quad (x, y)=1 \tag{10}$$

仅有整数解$x^2=1$，$y=0$和$x=0$，$y^2=1$。

证 设(10)存在$xy\neq0$的整数解，可设$x>0$，$y>0$，$y\equiv1 \pmod 2$且y是所有解中最小的。由(10)整理得$4z^2-(2x^2+y^2)^2=3y^4$，即

$$(2z+2x^2+y^2)(2z-2x^2-y^2)=3y^4 \tag{11}$$

由$(x, y)=1$易知$(2x^2+y^2, 3y)=1$，故$(2z+2x^2+y^2, 2z-2x^2-y^2)=1$。于是(11)给出

$$2z+2x^2+y^2=a^4,\quad 2z-2x^2-y^2=3b^4,\quad y=ab, \tag{12}$$

或

$$2z+2x^2+y^2=3a^4,\quad 2z-2x^2-y^2=b^4,\quad y=ab, \tag{13}$$

其中$a>0$，$b>0$且$(a, b)=1$。由(12)知

$$4x^2=a^4-3b^4-2y^2=a^4-2a^2b^2-3b^4,$$

由$y\equiv 1 \pmod 2$知$2\nmid ab$，故上式给出$4x^2\equiv -4 \pmod{16}$，这不可能。而由（13）得

$$4x^2=3a^4-2a^2b^2-b^4=(a^2-b^2)(3a^2+b^2),$$

由于$x>0$，故上式给出

$$a^2-b^2=c^2,\quad 3a^2+b^2=4d^2,$$

且因为$2\nmid ab$，$(a,\ b)=1$，故由$a^2-b^2=c^2$可得

$$a=p^2+q^2,\quad b=p^2-q^2,\quad p>q>0,\quad (p,\ q)=1,$$

代入$3a^2+b^2=4d^2$得出

$$p^4+p^2q^2+q^4=d^2,$$

这给出p，q，d是方程(10)的解，且$0<p<\sqrt{a}$，$0<q<\sqrt{a}$推出$0<p<y$，$0<q<y$，与y是所有解中最小的假设矛盾。证毕。

例 7 丢番图方程

$$x^4-x^2y^2+y^4=z^2,\quad (x,\ y)=1 \tag{14}$$

仅有整数解$x^2=1$，$y=0$；$x=0$，$y^2=1$和$x^2=y^2=1$。

证 (14)可整理成

$$(x^2-y^2)^2+x^2y^2=z^2。\tag{15}$$

情形1：x，y一奇一偶，则除去$x=0$，$y^2=1$和$x^2=1$，$y=0$可设$x>y>0$，且xy是(14)所有正整数解中最小的。于是(15)式给出

$$x^2-y^2=a^2-b^2,\quad xy=2ab,\quad (a,\ b)=1,\quad a>b>0, \tag{16}$$

设$d_1=(x,\ b)$，$d_2=(y,\ a)$，则

$$x=d_1x_1,\quad b=d_1b_1,\quad y=d_2y_1,\quad a=d_2a_1,\quad x_1y_1=2a_1b_1,$$

因为$(x_1,\ b_1)=1$，$(y_1,\ a_1)=1$，所以$(x_1,\ y_1)=(2a_1,\ b_1)$或$(a_1,\ 2b_1)$。因此

$$x=2a_1d_1,\quad b=d_1b_1,\quad y=d_2b_1,\quad a=d_2a_1, \tag{17}$$

或

$$x=a_1d_1,\ b=d_1b_1,\ y=2d_2b_1,\ a=d_2a_1。\qquad (18)$$

把（17）代入（16）式，则有

$$4a_1^2d_1^2-d_2^2b_1^2=d_2^2a_1^2-d_1^2b_1^2,$$

整理得

$$d_1^2(4a_1^2+b_1^2)=d_2^2(a_1^2+b_1^2)。\qquad (19)$$

因为 $a_1^2+b_1^2\not\equiv 0 \pmod 3$ 和 $(a_1,b_1)=1$，故 $(4a_1^2+b_1^2,\ a_1^2+b_1^2)=1$。所以（19）给出

$$a_1^2+b_1^2=u^2,\ 4a_1^2+b_1^2=v^2。$$

对上两式不妨设 $2\nmid b_1$（因为$2|b_1$时，令$b_1=2b_1'$，则上两式化为$a_1^2+4b_1'^2=u^2$，$a_1^2+b_1'^2=(\frac{v}{2})^2$），于是从$4a_1^2+b_1^2=v^2$可得$a_1=pq$,$b_1=p^2-q^2$,代入$a_1^2+b_1^2=u^2$得 $p^4-p^2q^2+q^4=u^2$。但$pq=a_1\leqslant a\leqslant\frac{xy}{2}<xy$，且$p$，$q$ 一奇一偶，矛盾。

再把（18）代入（16）式得

$$a_1^2d_1^2-4d_2^2b_1^2=d_2^2a_1^2-d_1^2b_1^2,$$

推出

$$d_1^2(a_1^2+b_1^2)=d_2^2(a_1^2+4b_1^2),$$

此与前类似，仍不可能。

情形2：x，y同奇，则除去 $x^2=y^2=1$可设 $x>y>0$。由（15）给出

$$x^2-y^2=2ab,\ xy=a^2-b^2,\ (a,\ b)=1。$$

其中 a，b 一奇一偶。于是推得

$$a^4-a^2b^2+b^4=\left(\frac{x^2+y^2}{2}\right)^2,$$

此由情形1的讨论知不可能。证毕。

由例7可推出：丢番图方程

$$x^4+14x^2y^2+y^4=z^2,\ (x,\ y)=1 \qquad (20)$$

仅有整数解$xy=0$，±1。这是因为，令$x+y=a$，$x-y=b$，则 $x=\frac{a+b}{2}$，$y=\frac{a-b}{2}$代入（20）得

$$a^4-a^2b^2+b^4=z^2。\qquad (21)$$

由于a，b同奇同偶，故$(a,\ b)=1$或2。在$(a,\ b)=1$时，由例7知仅有$a^2=b^2=1$。从而给出$xy=\frac{a^2-b^2}{4}=0$。而在$(a,\ b)=2$时，（21）化为，

$$\left(\frac{a}{2}\right)^4-\left(\frac{a}{2}\right)^2\left(\frac{b}{2}\right)^2+\left(\frac{b}{2}\right)^4=\left(\frac{z}{4}\right)^2,$$

故由例7知仅有$\left(\frac{a}{2}\right)^2=1$，$\frac{b}{2}=0$；$\frac{a}{2}=0$，$\left(\frac{b}{2}\right)^2=1$和$\left(\frac{a}{2}\right)^2=\left(\frac{b}{2}\right)^2=1$。此分别给出$xy=1$，$-1$和0。

习　　题

1. 证明丢番图方程$x^4-y^4=2z^2$无$z\neq0$的整数解。

2. 设p是奇素数，且$p\equiv\pm3\pmod 8$，则丢番图方程$x^4+2py^4=z^2$，$(x,\ y)=1$，$y\neq0$无整数解。

3. 设$p\equiv3\pmod 8$是奇素数，证明丢番图方程$x^4=y^4+pz^2$无$z\neq0$的整数解。

4. 证明丢番图方程$x^3+y^3+z^3=0$无$xyz\neq0$的整数解。

§4　比较素数幂法

比较素数幂法，是在丢番图方程两端比较某素数p的最

高方幂，以此来导致矛盾。例如，设有丢番图方程

$$f(x_1, \cdots, x_m)=g(y_1, \cdots, y_n), \qquad (1)$$

对某素数p，如果我们能够证明 $p^s\|f$，$p^t\|g$，且 $s\neq t$，则方程(1)无整数解。或者把方程(1)变形为

$$f-g=0, \qquad (2)$$

左端$p^s\|(f-g)$，s是一个有限正整数，而右端是0，从而导致矛盾。

这种方法实际上也是一种同余法。例如，如果$p^s\|(f-g)$，则对方程(2) 取模 p^{s+1}可导致矛盾。但比较素数幂法毕竟给我们提供了一个解决问题的思路。

例 1 丢番图方程

$$x^2+1=4y \qquad (3)$$

无整数解。

证 由(3)显然 $2\nmid x$，故 $2\|x^2+1$。因此比较(3)式两端含2的方幂知，方程(3)无整数解。

例 2 设p 为奇素数，则丢番图方程

$$\frac{x^p-y^p}{x-y}=p^2z,\ (x,\ y)=1 \qquad (4)$$

无整数解。

证 由(4)知

$$x^p-y^p=p^2z(x-y),$$

故$x-y\equiv 0 \pmod p$，令 $x-y=k$，则

$$\frac{x^p-y^p}{x-y}=\frac{(y+k)^p-y^p}{k}=\sum_{i=1}^{p}\binom{p}{i}y^{p-i}k^{i-1}。 \qquad (5)$$

现在，我们来比较(5) 式两端含 p的最高方幂。由于 $p\mid x-y=k$，且由 $(x,\ y)=1$知 $p\nmid y$，故

$$\sum_{i=1}^{p}\binom{p}{i}y^{p-i}k^{i-1}\equiv\binom{p}{1}y^{p-1} \pmod{p^2},$$

即 $p\| \sum_{i=1}^{p}\binom{p}{i}y^{p-i}k^{i-1}$，但(5) 式右端 $=p^2z$，这就证明方程(4)无整数解。

例 3 丢番图方程

$$(x+2)^{2m}=x^n+2 \tag{6}$$

无正整数解 x, m, n。

证 由(6)显然 $n>1$，$2\nmid x$。如果 $2|n$，则对(6) 取模4知无解。故可设 $2\nmid n$。

改写方程(6)为

$$(x+2)^{2m}-1=x^n+1, \tag{7}$$

令 $x+1=2^s x_1$，$s\geqslant 1$，$2\nmid x_1$。我们来比较 (7) 两端含2的方幂。因为

$$(x+2)^{2m}-1=(2^s x_1+1)^{2m}-1\equiv 0 \pmod{2^{s+1}},$$

$$x^n+1=x\cdot(2^s x_1-1)^{n-1}+1\equiv x+1=2^s x_1 \pmod{2^{s+1}},$$

故如果设 $2^u\|(x+2)^{2m}-1$，$2^v\|x^n+1$，则有 $u>v$。因此(7)不成立，证毕。

例 4 丢番图方程

$$(x+1)^y-x^z=1,\quad y>1,\quad z>1 \tag{8}$$

除 $x=2$，$y=2$，$z=3$ 外，无正整数解。

证 显然 $y<z$，由(8) 式得

$$\sum_{i=1}^{y}\binom{y}{i}x^{i-1}-x^{z-1}=0。 \tag{9}$$

如果 x 含有奇素数因子 p，可设 $x=p^a x_1$，$a\geqslant 1$，$p\nmid x_1$。由(9)式知 $p|y$。设 $y=p^b y_1$，$b\geqslant 1$，$p\nmid y_1$，我们来比较(9)式各项中所含 p 的方幂。

因为由 $y<z$ 知

$$b<1+b\cdot 2^{b-1}\leqslant(1+2)^b-1\leqslant p^b-1\leqslant a(p^b y_1-1)=$$

$a(y-1)<a(z-1)$，

所以p在x^{y-1}和x^{z-1}中出现的方幂都大于b。对于

$$T_i=\binom{y}{i}x^{i-1}$$

$$=\frac{y}{i}\binom{y-1}{i-1}x^{i-1}=\frac{p^b y_1}{i}\binom{y-1}{i-1}(p^a x_1)^{i-1}, i>1,$$

设$p^c\|i$，则T_i中含p的方幂至少是

$$\lambda=b+a(i-1)-c。$$

如果$c=0$，则$\lambda>b$；如果$c>0$，则$i\geqslant p^c>c+1$，故$\lambda>b+ac-c\geqslant b$。因此在(9)式中，除$y=p^b y_1$，$p\nmid y_1$外，其他所有项均能被$p^{b+1}$整除，这推出(9)式左端含$p$的最高方幂为$b$，与右端为0矛盾。

如果x不含奇素数因子，则$x=2^s$，$s>0$，(8)式成为

$$(2^s+1)^y-2^{sz}=1,\quad y>1,\quad z>1。\qquad (10)$$

由于在$2\nmid y$时，$(2^s+1)^y\equiv 2^s+1\pmod{2^{s+1}}$，故对(10)取模$2^{s+1}$知$2|y$。设$y=2y_1$，$y_1>0$，则(10)给出

$$(2^s+1)^{y_1}-1=2^k,\quad (2^s+1)^{y_1}+1=2^l,\quad k+l=sz,\qquad (11)$$

由前两式得$2^l-2^k=2$，此给出$k=1$，$l=2$，故由(11)给出$(2^s+1)^{y_1}=3$，$sz=3$，从而$y_1=1$，$s=1$，$z=3$。即给出方程(8)仅有正整数解$x=2$，$y=2$，$z=3$。证毕。

例 5 设p为奇素数，则丢番图方程

$$(x+y\sqrt{-2})^p+(x-y\sqrt{-2})^p=2\qquad (12)$$

在$2|y$时，仅有整数解$x=1$，$y=0$。

证 由方程(12)得

$$1=\frac{(x+y\sqrt{-2})^p+(x-y\sqrt{-2})^p}{2}$$

$$=\sum_{i=0}^{p}\frac{1+(-1)^i}{2}\binom{p}{i}x^{p-i}(y\sqrt{-2})^i$$

$$= \sum_{\substack{0 \leqslant i \leqslant p \\ 2 \mid i}} \binom{p}{i} x^{p-i} (y\sqrt{-2})^i$$

$$= \sum_{0 \leqslant i \leqslant \frac{p-1}{2}} \binom{p}{2i} x^{p-2i} (y\sqrt{-2})^{2i}, \tag{13}$$

由此知 $x \mid 1$，所以 $x = \pm 1$。

如果 $x = -1$，则(13)给出

$$-2 = \sum_{1 \leqslant i \leqslant \frac{p-1}{2}} \binom{p}{2i} (y\sqrt{-2})^{2i},$$

但 $p \mid \binom{p}{2i}$ $\left(1 \leqslant i \leqslant \frac{p-1}{2}\right)$，故上式给出 $p \mid 2$的矛盾结果。

如果 $x = 1$，则(13)给出

$$0 = \sum_{1 \leqslant i \leqslant \frac{p-1}{2}} \binom{p}{2i} (y\sqrt{-2})^{2i}。 \tag{14}$$

如果$y \neq 0$，则设$y = 2^{\alpha} y_1$，$2 \nmid y_1$，$\alpha > 0$。现在考察(14)的右端含 2 的最高方幂。由

$$\binom{p}{2i} (y\sqrt{-2})^{2i} = \frac{p(p-1)}{(2i)(2i-1)} \binom{p-2}{2i-2} (2^{\alpha} y_1 \sqrt{-2})^{2i}$$

可知，若设 $2^r \| p-1$，$2^{\beta} \| i$，则上式含 2 的方幂至少是 $r + (2\alpha + 1)i - (\beta + 1)$。

由于$i \geqslant 2^{\beta} \geqslant \beta + 1$，故$r + (2\alpha + 1)i - (\beta + 1) \geqslant r + 2\alpha i$。

因此，如设$2^{s_i} \| \binom{p}{2i} (y\sqrt{-2})^{2i}$ $\left(1 \leqslant i \leqslant \frac{p-1}{2}\right)$，则 $s_i > s_1$ $(i > 1)$，此即 $2^{s_1} \| \sum_{1 \leqslant i \leqslant \frac{p-1}{2}} \binom{p}{2i} (y\sqrt{-2})^{2i}$，故(14)在$y \neq 0$时不成立。这就证明了方程(12)在$2 \mid y$时仅有整数解$x = 1$，$y = 0$。证毕。

如果使用二次剩余法（§5）或Pell方程法（§6）还可以证明：方程(12)在$2 \nmid y$ 时仅有整数解 $x = |y| = 1, p = 5$。

利用比较素数幂法，常常会收到出乎意料的结果。这种

方法多半是用在二项式展开后的情形，而这种情形常常出现在代数整环中考虑的丢番图方程上（参见第三章），故比较素数幂法常常是与其他初等的或高等的方法联合使用，才可能解决一些比较困难的丢番图问题。

习　　题

1. 证明丢番图方程$2^x-3^y=1$ 仅有整数解$x=1, y=0$和 $x=2$，$y=1$ 。

2. 证明丢番图方程$1^{2n}+3^{2n}+\cdots+(2^a-1)^{2n}=2^a k$无正整数解 a，k，n。
（提示：证明左端含 2 的最高方幂为 $a-1$）。

3. 设$h=2^{s+3}l-1$或$2^{s+3}l$，$s\geqslant 0, 2\nmid l$。证明丢番图方程

$$\sum_{j=1}^{h} j^{2n+1}=2^{2s+4}(2k-1)$$

无正整数解。
（提示：利用

$$\sum_{j=1}^{h} j^{n}=\begin{cases}\dfrac{h^2(h+1)^2}{(n+1)!}f_n(h), & \text{当}2\nmid n,\ n>1;\\ \dfrac{h(h+1)(2h+1)}{(n+1)!}\varphi_n(h), & \text{当}2\mid n, n>0.\end{cases}$$

其中 $f_n(h)$和 $\varphi_n(h)$都是 h 的整系数多项式）。

4. 设 p为奇素数，则丢番图方程

$$(x+y\sqrt{-1})^p+(x-y\sqrt{-1})^p=2$$

在 $2\mid y$时仅有整数解$x=1$，$y=0$ 。

§5 二次剩余法

二次剩余法是解丢番图方程中最有力的初等方法之一，

它的主要手段是对丢番图方程取模M（$2\nmid M>1$），然后利用Jacobi符号的互反律来制造矛盾。这种方法的依据是，如果$y^2=f(x_1,\ \cdots,\ x_s)$有解，则对任意奇数模$M$（$M>1$），同余式$y^2\equiv f(x_1,\ \cdots,\ x_s)\pmod{M}$必有解，在$(M,\ y)=1$时推出Jacobi符号$\left(\frac{f(x_1,\ \cdots,\ x_s)}{M}\right)=1$。如果我们能选择$M$使得$\left(\frac{f(x_1,\ \cdots,\ x_s)}{M}\right)=-1$，则推出方程$y^2=f(x_1,\cdots,x_s)$无解。

这种方法的关键是根据$f(x_1,\ \cdots,\ x_s)$的特点选择$M=g(x_1,\ \cdots,\ x_s)>1$，$2\nmid M$来计算Jacobi符号$\left(\frac{f(x_1,\ \cdots,\ x_s)}{g(x_1,\ \cdots,\ x_s)}\right)$。例如，对于

$$A(n)=\frac{x^n-y^n}{x-y},\quad x\neq y,\quad (x,\ y)=1\text{且}x>0,\ y>0,$$

我们有下述例子。

例 1 设m，n都是>2的正奇数，$(m,\ n)=1$，则

1） 如果$x+y\equiv0\pmod 4$，则$\left(\frac{A(m)}{A(n)}\right)=1$；

2） 如果$xy\equiv0\pmod 4$，则$\left(\frac{A(m)}{A(n)}\right)=1$。

证 不妨设$m>n\geqslant3$，由于$x+y\equiv0\pmod4$或$xy\equiv0\pmod 4$，故在$2\nmid t$时

$$A(t)=x^{t-1}+x^{t-2}y+\cdots+xy^{t-2}+y^{t-1}\equiv1\pmod 4。$$

对于$m>n$，必有正奇数$r<n$使得

$$m=2kn+r\text{或}\ m=2kn-r,$$

如果$m=2kn+r$，由于$x^n-y^n=(x-y)\ A(n)$，我们得到

$$A(m)=\frac{x^{2kn+r}-y^{2kn+r}}{x-y}$$

$$=\frac{((x-y)A(n)+y^{n})^{2k}x^{r}-y^{2kn+r}}{x-y}$$

$$\equiv y^{2kn}A(r)\pmod{A(n)},$$

由于 $(A(m),\ A(n))=A((m,\ n))=A(1)=1$，故上式给出

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{A(r)}{A(n)}\right);$$

如果 $m=2kn-r$，由于

$A(m)=x^{n-r}A(n(2k-1))+y^{m-n}A(n)-y^{m-n}x^{n-r}A(r)$，

注意到 $A(n)\mid A(n(2k-1))$，$A(n)\equiv1\pmod 4$ 及 $m-n$ 和 $n-r$ 都是偶数，上式给出

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{-y^{m-n}x^{n-r}A(r)}{A(n)}\right)=\left(\frac{A(r)}{A(n)}\right)。$$

这就证明当 $m=2kn+\varepsilon r$ $(\varepsilon=\pm1)$ 时

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{A(r)}{A(n)}\right)。$$

故对于 n，r，

$$n=2k_1r+\varepsilon_1r_1,\quad 0<r_1<r,$$

$$r=2k_2r_1+\varepsilon_2r_2,\quad 0<r_2<r_1,$$

$$\cdots\cdots\cdots\cdots$$

$$r_{s-1}=2k_{s+1}r_s+\varepsilon_{s+1}r_{s+1},\quad 0<r_{s+1}<r_s,$$

$$r_s=k_{s+2}r_{s+1},$$

其中 $\varepsilon_i\in\{-1,\ 1\}$ $(i=1,\ 2,\ \cdots,\ s+1)$，$2\nmid r_i$ $(i=1,\ 2,\cdots,\ s+1)$ 且由 $(m,\ n)=1$ 知 $r_{s+1}=1$，我们有

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{A(r)}{A(n)}\right)=\left(\frac{A(n)}{A(r)}\right)=\left(\frac{A(r_1)}{A(r)}\right)=\left(\frac{A(r)}{A(r_1)}\right)=$$

$\left(\frac{A(r_2)}{A(r_1)}\right)=\cdots=\left(\frac{A(r_{s-1})}{A(r_s)}\right)=\left(\frac{A(1)}{A(r_s)}\right)=\left(\frac{1}{A(r_s)}\right)=1$ 。证毕。由例1可以推出

例 2 设p是奇素数，则丢番图方程

$$y^2=p\frac{x_1^p-x_2^p}{x_1-x_2},\quad (x_1,\ x_2)=1 \tag{1}$$

在$x_1+x_2\equiv 0\pmod 4$或$x_1x_2\equiv 0\pmod 4$时无整数解。

证 记$A(p)=\dfrac{x_1^p-x_2^p}{x_1-x_2}$，则由例1知，在$x_1+x_2\equiv 0$ $\pmod 4$或$x_1x_2\equiv 0\pmod 4$时，对任意奇素数$q\neq p$，均有$\left(\dfrac{A(p)}{A(q)}\right)=1$，于是，我们可选$q$满足$\left(\dfrac{q}{p}\right)=-1$。如果方程(1)有整数解，必有

$$y^2\equiv pA(p)\pmod{A(q)},$$

此给出

$$1=\left(\frac{pA(p)}{A(q)}\right)=\left(\frac{p}{A(q)}\right)\left(\frac{A(p)}{A(q)}\right)=\left(\frac{p}{A(q)}\right)=\left(\frac{A(q)}{p}\right)。$$

由于(1)给出$p|y$，故设$y=py_1$，由(1)得出

$$p(x_1-x_2)y_1^2=x_1^p-x_2^p,$$

取模p知$x_1\equiv x_2\pmod p$，故

$$A(q)=\frac{x_1^q-x_2^q}{x_1-x_2}=x_1^{q-1}+x_1^{q-2}x_2+\cdots+x_1x_2^{q-2}+x_2^{q-1}$$
$$\equiv qx_1^{q-1}\pmod p。$$

所以

$$1=\left(\frac{A(q)}{p}\right)=\left(\frac{qx_1^{q-1}}{p}\right)=\left(\frac{q}{p}\right)=-1,$$

这是不可能的。证毕。

对于$A(n)$，例 1 给出 $xy\equiv 0, 3 \pmod 4$ 的情形。当 $xy\equiv 1 \pmod 4$ 时，还可证明下面的结论。

例 3 设m，n都是正奇数，$(m, n)=1$，$n>1$，如果 $xy\equiv 1 \pmod 4$，则$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{m}{n}\right)$。

证 对m使用归纳法。$m=1$时，结论显然成立，现设$<m$结论成立，在m时，如果$m>n$，则存在正奇数$r<n$使得$m=2kn+r$或$m=2kn-r$。

如果$m=2kn+r$，则由例 1 证明显然有

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{A(r)}{A(n)}\right),$$

故由归纳假设及$r<n<m$知，上式给出

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{r}{n}\right)=\left(\frac{m}{n}\right);$$

如果$m=2kn-r$，则由例1的证明知

$$A(m)\equiv -y^{m-n}x^{n-r}A(r) \pmod{A(n)},$$

又在 $xy\equiv 1 \pmod 4$ 时易知

$$A(n)\equiv n \pmod 4,$$

故由 $m-n$，$n-r$ 均为偶数和归纳假设知

$$\left(\frac{A(m)}{A(n)}\right)=\left(\frac{-y^{m-n}x^{n-r}A(r)}{A(n)}\right)=(-1)^{\frac{A(n)-1}{2}}\left(\frac{A(r)}{A(n)}\right)$$

$$=(-1)^{\frac{n-1}{2}}\left(\frac{r}{n}\right)=\left(\frac{-r}{n}\right)=\left(\frac{m}{n}\right)。$$

如果$m<n$，则由前面已经证明的结论知

$$\left(\frac{A(m)}{A(n)}\right)=(-1)^{\frac{A(m)-1}{2}\cdot\frac{A(n)-1}{2}}\left(\frac{A(n)}{A(m)}\right)$$

$$=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)，\text{证毕。}$$

利用例 3 立即推出 Fermat 方程偶指数的第一情形成立，即有

例 4 设p是奇素数，则丢番图方程

$$x^{2p}+y^{2p}=z^{2p},\quad (x,\ y)=1 \tag{2}$$

在$2p\nmid xyz$时无正整数解。

证 由方程(2)知x，y一奇一偶。不妨设x为偶数，则y，z为奇数。现改写(2)为

$$x^{2p}=(z^2-y^2)\cdot\frac{z^{2p}-y^{2p}}{z^2-y^2}, \tag{3}$$

由于$\left(z^2-y^2,\ \frac{z^{2p}-y^{2p}}{z^2-y^2}\right)=1$ 或 p，且如果是后者已有

$2p\mid x$，与$2p\nmid xyz$不符，故$\left(z^2-y^2,\ \frac{z^{2p}-y^{2p}}{z^2-y^2}\right)=1$，于是(3)式给出

$$\frac{z^{2p}-y^{2p}}{z^2-y^2}=(x_1^p)^2 \tag{4}$$

这里$x_1\mid x$。由于z，y均为奇数，故 $z^2\cdot y^2\equiv 1 \pmod 4$ 因此，由例 3 知对任意$q\neq p$，(4) 式均推出

$$\left(\frac{p}{q}\right)=1,$$

而这是不可能的。因为p是素数，存在某些奇素数q使得$\left(\frac{p}{q}\right)=-1$。证毕。

对例 4 的进一步推广，可以得到

例 5 设$D>0$，D无平方因子且不被$2mp+1$形素数整除。如果丢番图方程

$$x^p-y^p=Dz^2,\quad (x,\ y)=1 \tag{5}$$

有整数解，则在$2|z$时必有 $p|z$，$2\nmid z$时必有 $p\nmid z$。

二次剩余法是柯召[1]首先用来研究并解决Catalan 方程$x^2-1=y^p$（p为奇素数）的一种初等方法，后来在1977 年G. Terjanian[2]利用这种方法得到了上述例 4 的结论，曹珍富[3]证明了上面的例1，例2和例5。这种方法我们在后面§7中还将看到，在与递推序列的性质联合使用时可以解决更为广泛的丢番图问题。例如，1983年，A. Rotkiewicz[4] 把上述$A(n)$换为Lehmer数P_n 也得出了类似的结果。设

$$P_n(\alpha, \beta)=\begin{cases}\dfrac{\alpha^n-\beta^n}{\alpha-\beta}, & \text{当 } 2\nmid n\text{时；}\\[2mm] \dfrac{\alpha^n-\beta^n}{\alpha^2-\beta^2}, & \text{当 } 2|n\text{时。}\end{cases}$$

其中 α，β 是方程$z^2-\sqrt{L}\,z+M=0$ 的两个根，$L>0$ 和M均为整数。则有如下的结果：

例 6 设$2\nmid mn$，$K=L-4M>0$，则有

1） 如果 $4|L$，$M\equiv1 \pmod 4$，$\left(\dfrac{L}{M}\right)=1$ 或$4|M$，$L\equiv3 \pmod 4$，$\left(\dfrac{M}{L}\right)=1$ ，则$\left(\dfrac{P_n}{P_m}\right)=\left(\dfrac{n}{m}\right)$；

2） 如果 $4|L$，$M\equiv3 \pmod 4$，$\left(\dfrac{L}{M}\right)=1$ 或$4|M$，$L\equiv1 \pmod 4$，$\left(\dfrac{M}{L}\right)=1$ ，则$\left(\dfrac{P_n}{P_m}\right)=1$；

3） 如果$2\|M$，$L\equiv1 \pmod 4$，$\left(\dfrac{M}{L}\right)=1$ ，则$\left(\dfrac{P_n}{P_m}\right)=(-1)^\lambda$，这里 λ 是把$\dfrac{n}{m}$写成连分数的项数，即$\dfrac{n}{m}=a_1+$

$\frac{1|}{|a_2} + \cdots + \frac{1|}{|a_\lambda}$，$a_\lambda > 1$ 。

为了把例 6 更好地应用到丢番图方程中去，A.Rotkiewicz 还提出了如下的问题：

设$n>3$，$n \neq 9$是一个给定的奇数，问是否存在奇数m 使得$\left(\frac{m}{n}\right) = (-1)^\lambda$和$\frac{n}{m} = a_1 + \frac{1|}{|a_2} + \cdots + \frac{1|}{|a_\lambda}$，$a_\lambda > 1$ ？这个问题在1985年已由曹珍富[5]给出了肯定的回答。

习　　题

1． 证明 Catalan 方程$x^2 - 1 = y^p$（$p>3$ 是素数）在$p|x$时 无正整数解。

2． 证明丢番图方 程 $3^{2^n-1} + 2y^2 = n(2y)^2 + 1$ 除开$n=1$，$y=1$ 外无其他的正整数解。

3． 设 p 为奇素数，如果丢番图方程 $x^p + 1 = 2y^p$ 有$xy \neq 0$的整数解，则有$2 \nmid y$且$p | y-1$，

4． 如果 $n \equiv 0$，1（mod4），则方程$\binom{n}{2} = y^k$，$k>2$无正整数解。

§6 Pell 方 程 法

通常所说的Pell方程是指形如$x^2 - Dy^2 = \pm 1$ 的二元二次丢番图方程，这里$D>0$，且不是平方数。所谓Pell 方程法就是把所求问题化为Pell方程的形式，利用Pell 方程的结果来制造矛盾。一般说来，利用Pell 方程的解法，可以求出一个丢番图方程（只要能化为Pell方程的形式）的全部解。

下面我们首先列出Pell方程的主要结果（它们的证明放在后面章节中）；其次，利用Pell方程来解决一些丢番图方程的问题。以下恒设$D>0$ 且不是平方数。

Ⅰ. Pell 方程

$$x^2-Dy^2=1 \qquad (1)$$

有无限多组正整数解。设$x=x_0$，$y=y_0$ 是(1)的所有正整数解x，y中使 $x+y\sqrt{D}$为最小的一组正整数解（称 $x_0+y_0\sqrt{D}$为(1)的基本解），则Pell 方程(1)的全部正整数解由

$$x+y\sqrt{D}=(x_0+y_0\sqrt{D})^n$$

表出，其中 n 是任意正整数。

Ⅱ. Pell 方程

$$x^2-Dy^2=-1 \qquad (2)$$

不是对任意D都有解的。例如D含有$4k+3$形的素因子时(2)显然无解。但是，如果方程(2) 有解，设$a+b\sqrt{D}$是它的基本解（$a>0$，$b>0$），则方程(2) 的全部正整数解可表为

$$x+y\sqrt{D}=(a+b\sqrt{D})^{2n+1},$$

其中 n 是非负整数。

与Pell方程直接发生关系的还有一些方程，这些方程在利用Pell方程解其他丢番图方程时，也显示了重要作用。

Ⅲ. 方程

$$x^2-Dy^2=4 \qquad (3)$$

有无限多组解。设 $c+d\sqrt{D}$为(3)的基本解($c>0$，$d>0$)，则(3)的全部正整数解由

$$\frac{x+y\sqrt{D}}{2}=\left(\frac{c+d\sqrt{D}}{2}\right)^n$$

表出，其中 n 是任意正整数。

Ⅳ．方程

$$x^2-Dy^2=-4 \tag{4}$$

如果有解，设 $e+f\sqrt{D}$ 是(4) 的基本解（$e>0$，$f>0$）。则方程(4)的全部正整数解由

$$\frac{x+y\sqrt{D}}{2}=\left(\frac{e+f\sqrt{D}}{2}\right)^{2n+1}$$

表出，其中 n 是非负整数。

在利用 Pell 方程解题时，用到的事实主要是方程(1)～(4)的基本解之间的关系。对此，我们有：

Ⅴ．设 $\varepsilon=x_0+y_0\sqrt{D}$，$\delta=a+b\sqrt{D}$，$\alpha=\dfrac{c+d\sqrt{D}}{2}$，$\beta=\dfrac{e+f\sqrt{D}}{2}$，则有

$$\varepsilon=\delta^2=\begin{cases}\alpha, & \text{当} c\equiv d\equiv 0 \pmod 2;\\ \alpha^3, & \text{当} c\equiv d\equiv 1 \pmod 2。\end{cases}$$

$$\delta=\begin{cases}\beta, & \text{当} e\equiv f\equiv 0 \pmod 2;\\ \beta^3, & \text{当} e\equiv f\equiv 1 \pmod 2。\end{cases}$$

Ⅵ．如果方程 $x^2-Dy^2=2\eta$（$\eta=\pm1$）有整数解，可设 $\lambda_\eta=g+h\sqrt{D}$ 为其基本解，则在 $D>2$ 时有

$$\varepsilon=\frac{1}{2}\lambda_\eta^2,\quad \overline{\varepsilon}=\frac{1}{2}\overline{\lambda}_\eta^2\left(\overline{\lambda}_\eta=g-h\sqrt{D}\right),$$

且方程的全部正整数解可表为 $x+y\sqrt{D}=\dfrac{\lambda_\eta^{2n+1}}{2^n}$，$n\geqslant 0$。

现在我们举若干例子，用以说明Pell方程法的应用。

例 1　设 D 满足 $X^2-DY^2=-4$ 有奇数解 X，Y，则丢番图方程

$$4x^4-Dy^2=-1 \tag{5}$$

除开$D=5$，$x=y=1$，$D=13$，$x=2$，$y=5$ 和 $D=325$，$x=2$，$y=1$ 外，无其他的正整数解。

证 利用Pell方程(2)的结果可知，如果（5）有正整数解，则(5)给出

$$2x^2+y\sqrt{D}=(a+b\sqrt{D})^{2n+1},\quad n\geqslant 0。\tag{6}$$

现由$X^2-DY^2=-4$有奇数解知，$X^2-DY^2=-4$的基本解$e+f\sqrt{D}$满足$e\equiv f\equiv 1 \pmod 2$，故由V知$a+b\sqrt{D}=\beta^3$，于是(6)给出

$$2x^2+y\sqrt{D}=\beta^{3(2n+1)},\quad n\geqslant 0。$$

如果令$\overline{\beta}=\dfrac{e-f\sqrt{D}}{2}$，$\beta\overline{\beta}=-1$，则上式给出

$$\begin{aligned}(2x)^2&=\beta^{3(2n+1)}+\overline{\beta}^{3(2n+1)}\\&=(\beta^{2n+1}+\overline{\beta}^{2n+1})(\beta^{2(2n+1)}+\overline{\beta}^{2(2n+1)}+1),\\ &n\geqslant 0。\end{aligned}\tag{7}$$

因为对任意整数$m\geqslant 0$，$\beta^m+\overline{\beta}^m$都是整数，且$(\beta^{2n+1}+\overline{\beta}^{2n+1},\ \beta^{2(2n+1)}+\overline{\beta}^{2(2n+1)}+1)=1$或3，故(7)式给出

$$\beta^{2n+1}+\overline{\beta}^{2n+1}=s^2,\quad \beta^{2(2n+1)}+\overline{\beta}^{2(2n+1)}+1=t^2,\quad 2x=st,\tag{8}$$

或

$$\beta^{2n+1}+\overline{\beta}^{2n+1}=3s^2,\quad \beta^{2(2n+1)}+\overline{\beta}^{2(2n+1)}+1=3t^2,\quad 2x=3st,\tag{9}$$

其中$s>0$，$t>0$且$(s,t)=1$。因为

$$\beta^{2(2n+1)}+\overline{\beta}^{2(2n+1)}+1=(\beta^{2n+1}+\overline{\beta}^{2n+1})^2+3,$$

故在(8)时，有$s^4+3=t^2$，此给出$(t-s^2)(t+s^2)=3$，

故$t-s^2=1$，$t+s^2=3$，于是$t=2$，$s=1$。从$2x=st$知$x=1$，代入(5)知$D=5$，$y=1$，显然$D=5$时满足$X^2-DY^2=-4$有奇数解。而在(9)时有

$$(3s^2)^2+3=3t^2 \text{即} t^2-3s^4=1。\qquad (10)$$

W.Ljunggren[6]曾证明，丢番图方程

$$x^2-Dy^4=1$$

最多只有两组正整数解，现在已知(10)有两组正整数解$t=2$，$s=1$和$t=7$，$s=2$，故(10)仅有这两组正整数解，所以由$2x=3st$知，在$t=2$，$s=1$时$x=3$，代入(5)得$D=13$，$y=5$或$D=325$，$y=1$，当$D=13$或325时，方程$X^2-DY^2=-4$显然有奇数解。在$t=7$，$s=2$时，由$2x=3st$知$x=21$，代入(5)得$Dy^2=37\cdot5^2\cdot29^2$，而$X^2-37Y^2=-4$没有奇数解，故此时不可能。证毕。

例 2 设D满足$X^2-DY^2=2\eta$（$\eta=\pm1$）有整数解，则丢番图方程

$$x^4-Dy^2=1 \qquad (11)$$

除$D=6$，$x=7$，$y=20$外，无其他的正整数解。

证 在$D=2$时，(11)显然无正整数解(参见§2的例2)。现设$D>2$，则如果(11)有正整数解，必有

$$x^2+y\sqrt{D}=(x_0+y_0\sqrt{D})^n,\quad n>0$$

其中$x_0+y_0\sqrt{D}$为Pell方程$x^2-Dy^2=1$的基本解。由Ⅵ知，上式给出

$$x^2=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2}=\frac{\lambda_\eta^{2n}+\bar{\lambda}_\eta^{2n}}{2^{n+1}},$$

由此推出

$$x^2+\eta^n=\frac{\lambda_\eta^{2n}+\bar{\lambda}_\eta^{2n}+2(\lambda_\eta\bar{\lambda}_\eta)^n}{2^{n+1}}=\frac{(\lambda_\eta^n+\bar{\lambda}_\eta^n)^2}{2^{n+1}}。\qquad (12)$$

如果$2\nmid n$，则(12)给出

$$x^2+\eta=\left(\frac{\lambda_\eta^n+\bar{\lambda}_\eta^n}{2^{(n+1)/2}}\right)^2,$$

由此得出 $x=0$或1，代入(11)知，均非(11)的正整数解。

如果$2|n$，设$n=2m$，$m>0$，则(12)给出

$$x^2+1=2s^2, \tag{13}$$

其中

$$s=\frac{\lambda_\eta^{2m}+\bar{\lambda}_\eta^{2m}}{2^{m+1}}=\frac{(\lambda_\eta^m+\bar{\lambda}_\eta^m)^2}{2^{m+1}}-\eta^m=\begin{cases}t^2-\eta, & \text{当 } 2\nmid m;\\ 2t^2-1, & \text{当} 2|m。\end{cases}$$

如果$s=t^2-\eta$，则在$\eta=1$时，我们有$s\equiv 0,3 \pmod 4$，这和(13)式矛盾。于是$\eta=-1$。现在，(13)又是一个Pell方程，它的基本解是 $\rho=1+\sqrt{2}$，设$\bar{\rho}=1-\sqrt{2}$， 则由(13) 得

$$s=\frac{\rho^{2k+1}-\bar{\rho}^{2k+1}}{2\sqrt{2}}=t^2+1,\quad k\geqslant 0$$

由此可得

$$t^2=\frac{\rho^{2k+1}-\bar{\rho}^{2k+1}-(\rho-\bar{\rho})}{2\sqrt{2}}=$$

$$\begin{cases}(\rho^{2l+1}+\bar{\rho}^{2l+1})\left(\dfrac{\rho^{2l}-\bar{\rho}^{2l}}{2\sqrt{2}}\right), & \text{当}k=2l;\\ (\rho^{2l+1}+\bar{\rho}^{2l+1})\left(\dfrac{\rho^{2l+2}-\bar{\rho}^{2l+2}}{2\sqrt{2}}\right), & \text{当}k=2l+1。\end{cases} \tag{14}$$

因为

$$\frac{\rho^{2l+1}+\bar{\rho}^{2l+1}}{2}=\frac{\rho^{2l}+\bar{\rho}^{2l}}{2}+2\cdot\frac{\rho^{2l}-\bar{\rho}^{2l}}{2\sqrt{2}},$$

$$\frac{\rho^{2l+2}-\bar{\rho}^{2l+2}}{2\sqrt{2}}=\frac{\rho^{2l+1}-\bar{\rho}^{2l+1}}{2\sqrt{2}}+\frac{\rho^{2l+1}+\bar{\rho}^{2l+1}}{2},$$

故$\left(\rho^{2l+1}+\bar{\rho}^{2l+1},\ \frac{\rho^{2l}-\bar{\rho}^{2l}}{2\sqrt{2}}\right)=2$，$\left(\rho^{2l+1}+\bar{\rho}^{2l+1},\right.$

$\left.\frac{\rho^{2l+2}-\bar{\rho}^{2l+2}}{2\sqrt{2}}\right)=2$。于是由（14）式可得

$$\rho^{2l+1}+\bar{\rho}^{2l+1}=2t_1^2, \tag{15}$$

所以存在整数 $u=\frac{\rho^{2l+1}-\bar{\rho}^{2l+1}}{2\sqrt{2}}$，满足

$$t_1^4-2u^2=(-1)^{2l+1}=-1,$$

此由§3的例3知仅有$t_1^2=1$，故由（15）推出$l=0$，由(14)推出$t^2=0$或4，从而$s=1$或5，推出$x=1$或7，由（11）知$y=0$或20，故此时仅有正整数解$D=6$，$x=7$，$y=20$。

如果$s=2t^2-1$，则重复前面作法可知

$$2t^2=\begin{cases}(\rho^{2l+1}+\bar{\rho}^{2l+1})\left(\frac{\rho^{2l}-\bar{\rho}^{2l}}{2\sqrt{2}}\right), & 当k=2l;\\ (\rho^{2l+1}+\bar{\rho}^{2l+1})\left(\frac{\rho^{2l+2}-\bar{\rho}^{2l+2}}{2\sqrt{2}}\right), & 当k=2l+1。\end{cases}$$

由此仍推出（15）式，从而$l=0$，故$t^2=0$或2，此不可能。证毕。

例1和例2都是可以直接利用Pell方程求解的，而有些丢番图方程表面上并不能一下子看出使用Pell方程，这些方程的求解在未发现使用Pell方程以前，往往用初等方法很难解决。

例 3 设p是奇素数，则丢番图方程

$$x^2-1=y^p \tag{16}$$

如有正整数解，必有$2|y$，$p|x$。

证 首先$2|y$是显然的，因为$2\nmid y$时有$2|x$，（16）显然

不能成立（参见§2），现在来证明$p|x$。设$p\nmid x$，则由(16)整理得

$$(y+1)\frac{y^p+1}{y+1}=x^2,$$

由$p\nmid x$知$\left(y+1,\ \frac{y^p+1}{y+1}\right)=1$，所以上式给出

$$y+1=x_1^2,\ 2\nmid x_1|x,\ x_1>1,$$

把 $y=x_1^2-1$ 代入（16）式得

$$x^2-(x_1^2-1)[(x_1^2-1)^{\frac{p-1}{2}}]^2=1。\qquad (17)$$

由于 Pell 方程 $x^2-(x_1^2-1)y^2=1$ 的基本解是 $\varepsilon=x_1+\sqrt{x_1^2-1}$，故（17）给出

$$\begin{aligned}(x_1^2-1)^{\frac{p-1}{2}}&=\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{x_1^2-1}}\\&=\binom{n}{1}x_1^{n-1}+\binom{n}{3}x_1^{n-3}(\sqrt{x_1^2-1})^2\\&\quad+\cdots+\binom{n}{2m+1}x_1^{n-(2m+1)}(\sqrt{x_1^2-1})^{2m},\end{aligned}\qquad (18)$$

其中 $n=2m+1$或 $n=2m+2$，$m\geqslant0$。在 $n=2m+2$ 时，对（18）取模x_1给出 $(-1)^{\frac{p-1}{2}}\equiv0\pmod{x_1}$，这不可能。而在$n=2m+1$时，由于 $2\nmid x_1$，故（18）式的左边为偶数，但右端是奇数，也不可能。证毕。

例 3 的结论，对于彻底解决方程(16)，起了重要作用。

例 4 设p和$q=p+2$都是素数，则丢番图方程

$$q^m=p^n+2\qquad (19)$$

仅有正整数解 $m=n=1$。

证 显然，除$m=n=1$，可设$m>1$，$n>1$。如果$2|n$，

则在$p=3$时$q=5$，故对（19）取模5知无解；而在$p\neq 3$时，由$2|n$知$3|p^n+2$，（19）给出$q=3$，与$q=p+2$不符。如果$2\nmid n$，$2|m$，则由§4的例3知（19）无解。现设$2\nmid mn$，如（19）有解，则有

$$\left(\frac{(p+2)^m+p^n}{2}\right)^2-p(p+2)\left((p+2)^{\frac{m-1}{2}}p^{\frac{n-1}{2}}\right)^2=1。$$

（20）

显然，Pell方程$x^2-p(p+2)y^2=1$的基本解是$\varepsilon=p+1+\sqrt{p(p+2)}$，令$\bar{\varepsilon}=p+1-\sqrt{p(p+2)}$，则（20）给出

$$(p+2)^{\frac{m-1}{2}}p^{\frac{n-1}{2}}=\frac{\varepsilon^t-\bar{\varepsilon}^t}{\varepsilon-\bar{\varepsilon}},\quad t>0, \tag{21}$$

由于$2|t$时$\frac{\varepsilon^t-\bar{\varepsilon}^t}{\varepsilon-\bar{\varepsilon}}$是偶数，故(21)给出$2\nmid t$，于是$\frac{\varepsilon^t-\bar{\varepsilon}^t}{\varepsilon-\bar{\varepsilon}}=$

$$\binom{t}{1}(p+1)^{t-1}+\binom{t}{3}(p+1)^{t-3}\left(\sqrt{p(p+2)}\right)^2+\cdots+$$

$$\binom{t}{t-2}(p+1)^2\left(\sqrt{p(p+2)}\right)^{t-3}+\left(\sqrt{p(p+2)}\right)^{t-1},$$

给出

$$\frac{\varepsilon^t-\bar{\varepsilon}^t}{\varepsilon-\bar{\varepsilon}}\equiv t\pmod{p(p+2)}, \tag{22}$$

由$m>1$，$n>1$及（21）式知，上式给出$p(p+2)|t$，设$t=p(p+2)t_1$，则（21）给出

$$(p+2)^{\frac{m-1}{2}}p^{\frac{n-1}{2}}=\frac{(\varepsilon^{pt_1})^{p+2}-(\bar{\varepsilon}^{pt_1})^{p+2}}{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}\cdot\frac{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}{\varepsilon-\bar{\varepsilon}}。$$

（23）

我们来证明，对任意正整数a_1和奇素数$q=p+2$，都有

$$\left(\frac{\varepsilon^{qa_1}-\bar{\varepsilon}^{qa_1}}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}},\ \frac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}\right)=1\text{或}q\text{。}\qquad(24)$$

这是因为，设 $\varepsilon^{a_1}=u+v\sqrt{D}$ $(D=pq=p(p+2))$，则 $\bar{\varepsilon}^{a_1}=u-v\sqrt{D}$，$v=\dfrac{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}{\varepsilon-\bar{\varepsilon}}$，我们有

$$\frac{\varepsilon^{qa_1}-\bar{\varepsilon}^{qa_1}}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}=\binom{q}{1}u^{q-1}+\binom{q}{3}u^{q-3}(v\sqrt{D})^2+\cdots+(v\sqrt{D})^{q-1},$$

由此即得（24）式，而且由此看出 $q\|\dfrac{\varepsilon^{qa_1}-\bar{\varepsilon}^{qa_1}}{\varepsilon^{a_1}-\bar{\varepsilon}^{a_1}}$。另外，注意到 $p\mid\dfrac{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}{\varepsilon-\bar{\varepsilon}}$，由（23）式得出

$$\frac{(\varepsilon^{pt_1})^{p+2}-(\bar{\varepsilon}^{pt_1})^{p+2}}{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}=p+2,$$

$$\frac{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}{\varepsilon-\bar{\varepsilon}}=p^{\frac{n-1}{2}},\quad\frac{m-1}{2}=1,\qquad(25)$$

或

$$\frac{(\varepsilon^{pt_1})^{p+2}-(\bar{\varepsilon}^{pt_1})^{p+2}}{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}=p+2,$$

$$\frac{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}{\varepsilon-\bar{\varepsilon}}=p^{\frac{n-1}{2}}\cdot(p+2)^{\frac{m-1}{2}-1},\qquad(26)$$

但 $\dfrac{(\varepsilon^{pt_1})^{p-2}-(\bar{\varepsilon}^{pt_1})^{p+2}}{\varepsilon^{pt_1}-\bar{\varepsilon}^{pt_1}}>p+2$，故（25），（26）均不成立。证毕。

方程（19）称为 Hall 方程，它是从组合数学的差集理论中提出来的[7]。例 4 解决了它的一个重要情形。

从上面的例题我们看到，利用Pell方程可以干净利落地解决一些丢番图方程问题。有时，为了需要，还可以用来构

造一些丢番图方程的无穷多组解。例如，方程$z^2+1=x^3+y^3$有无穷多组整数解。这是因为，如果令$x=1+\omega$，$y=1-\omega$，则由$z^2+1=x^3+y^3$得出Pell方程 $z^2-6\omega^2=1$。高斯曾利用推广的 Pell 方程$x^2-Dy^2=c$（此方程如果有解，便有无穷多组解），证明了：设 $D=b^2-4ac>0$，D不是平方数，$\triangle=4acf+bde-ae^2-cd^2-fb^2\neq 0$，且设方程$ax^2+bxy+cy^2+dx+ey+f=0$ 有一组整数解，则该方程有无穷多组整数解。利用类似的方法，还可解决1970年S.W.Golomb提出的一系列幂数问题（参见习题6）。

把Pell方程的方法，用于求解Catalan 方程（16）以及著名的 Hall 方程（19），获得了一些重要结果，而且证明过程简洁明快[7][8]。可以相信，Pell方程法在其他的一些丢番图方程上能够继续产生作用。

习　　题

1． 如果$u^2-Dv^2=-1$有整数解，则丢番图方程 $x^4-Dy^2=1$的正整数解x，y不满足

$$x^2=\frac{\varepsilon^{2n}+\bar{\varepsilon}^{2n}}{2},\quad n>0,$$

这里ε是Pell方程 $x^2-Dy^2=1$ 的基本解。

2． 设方程$u^2-Dv^2=2\eta$（$\eta=\pm 1$）有整数解，则丢番图方程$x^6-Dy^2=1$ 除开$D=7$，$x=2$，$y=3$外，无其他的正整数解。

3． 设p是奇素数，如果丢番图方程$x^p-1=2y^2$有解，则除开$p=5$，$x=3$，$y=11$外，必有$p\mid y$。

4． 设$2\nmid mn$，且Pell方程$x^2-pqy^2=1$的基本解是$x_0+y_0\sqrt{pq}$，则 Hall 方程

$$q^m = p^n + 2,\ p,\ q \text{ 是素数},\ m>1,\ n>1,$$

有解的充要条件是 $x_0 = q^m - 1$，$y_0 = p^{\frac{n-1}{2}} q^{\frac{m-1}{2}}$。

5。 设$2\nmid mn$，p，q 均是奇素数，则丢番图方程

$$\frac{q^n - 1}{q - 1} = p^m,\ n>3,\ m>1$$

有解的充要条件是 Pell 方程 $x^2 - Dy^2 = 1$ 的基本解为 $q^n + (q-1)p^m + 2p^{\frac{m-1}{2}} q^{\frac{n-1}{2}} \sqrt{D}$，这里$D = pq(q-1)$。

6。 我们称正整数m为幂数，如果对m的任一素因子p，有$p^2 | m$。1970年，S.W.Golomb[9] 猜想：形如 $2(2a+1)$ $(a\geqslant 0)$ 的数不是两个幂数之差。请否定这个猜想。

§7 递推序列法

递推序列法是通过讨论递推序列的数论性质（主要是同余性质），然后利用各种手法（例如二次剩余法）来制造矛盾。在初等方法中，递推序列法显得特别困难。这个困难主要表现在：1)针对一个丢番图方程，怎样把它转化为递推序列问题？2) 如何根据方程的类型，研究递推序列的数论性质？研究哪些数论性质？3) 选择怎样的手法来制造矛盾？一般说来，即使1)～3)都有明确的思路，但要真正实现还有许多特殊的技巧。

例 1 丢番图方程$x^2 - 27y^4 = -2$仅有正整数解$x = 5$，$y = 1$。

证 先来解方程

$$V^2 - 3U^2 = -2。$$

由§6中的Ⅵ，这个方程的全部正整数解可表为

$$V_n+U_n\sqrt{3}=\frac{\lambda^{2n+1}}{2^n},\quad n\geqslant 0,\quad \lambda=1+\sqrt{3}。$$

令$\bar{\lambda}=1-\sqrt{3}$，则上式给出

$$U_n=\frac{\lambda^{2n+1}-\bar{\lambda}^{2n+1}}{2^n(\lambda-\bar{\lambda})},\quad n\geqslant 0。$$

于是，若方程 $x^2-27y^4=-2$ 有正整数解，必有

$$3y^2=U_n,\quad n\geqslant 0\ 。\tag{1}$$

容易验证U_n 是递推序列

$$U_{n+2}=4U_{n+1}-U_n,\quad U_0=1,\quad U_1=3\tag{2}$$

的解。现在我们来讨论U_n 的一些数论性质。记

$$\xi_r=\frac{\lambda^r-\bar{\lambda}^r}{\lambda-\bar{\lambda}},\quad \eta_r=\frac{\lambda^r+\bar{\lambda}^r}{\lambda+\bar{\lambda}},\quad r\geqslant 0,$$

则有

$$U_n=\frac{\xi_{2n+1}}{2^n},\tag{3}$$

$$\xi_{2r}=2\xi_r\eta_r,\tag{4}$$

$$\eta_{2r}=2\eta_r^2+(-1)^{r+1}2^r=6\xi_r^2+(-1)^r2^r,\tag{5}$$

$$\eta_{m+n}=\eta_m\eta_n+3\xi_m\xi_n,\tag{6}$$

$$\xi_{m+n}=\eta_m\xi_n+\eta_n\xi_m,\tag{7}$$

由（3）～（7）可推出

$$U_{n+r}\equiv(-1)^{r+1}U_n\pmod{\eta_r2^{-s}},\tag{8}$$

$$U_{n+2r}\equiv U_n\pmod{\eta_r2^{-s}},\tag{9}$$

其中$s=s(r)\geqslant 0$。为了便于讨论，一方面，从递推序列(2)能够得出：

表 I

n	0	1	2	3	4	5	6	7
U_n	1	3	11	41	153	571	2131	7953

表Ⅱ

t	2	3	4	6	8	12
η_t	$2\cdot2$	$2\cdot5$	$2^2\cdot7$	$2^4\cdot13$	$2^4\cdot97$	$2^6\cdot7\cdot193$

另一方面，从（8）式，如果$n=rk+r_0$，$0\leqslant r_0<r$，则在$2\nmid r$ 时有

$$U_n\equiv(-1)^{r+1}U_{n-r}=U_{n-r}\equiv\cdots\equiv U_{r_0}(\bmod \eta_r\cdot2^{-s})；$$

而在$2|r$ 时有

$$U_n\equiv\pm U_{r_0}\ (\bmod\ \eta_r\cdot2^{-s})。$$

利用（9）式，如果$n=2kr+r_0$，$0\leqslant r_0<r$，则有

$$U_n\equiv U_{r_0}\ (\bmod\ \eta_r\cdot2^{-s})。$$

现在我们来讨论（1）的解。

1） 在$n\equiv0$，2（mod3）时，（1）不成立。我们有

$$U_n\equiv U_0,\ U_2\ (\bmod\ \eta_3\cdot2^{-1}),$$

从表Ⅰ、表Ⅱ知$U_0=1$，$U_2=11$，$\eta_3\cdot2^{-1}=5$，此时如果（1）有解，则有

$$(3y)^2\equiv3,\ 3\cdot11\ (\bmod\ 5),$$

但$\left(\frac{3}{5}\right)=\left(\frac{3\cdot11}{5}\right)=-1$，矛盾。

2）在$n\equiv0$，2，5，7（mod8）时，（1）不成立。因为

$$U_n\equiv U_0,\ U_2,\ U_5,\ U_7\ (\bmod\ \eta_4\cdot2^{-2})$$

而从表Ⅰ、表Ⅱ知

$$\left(\frac{3U_n}{\eta_4\cdot2^{-2}}\right)=\left(\frac{3}{7}\right)=\left(\frac{3\cdot11}{7}\right)=\left(\frac{3\cdot571}{7}\right)=\left(\frac{3\cdot7953}{7}\right)=-1,$$

故（1）不成立。

3） $n\equiv3$，4（mod 8）时，（1）不成立。因为

$$U_n \equiv \pm U_3, \ \pm U_4 \pmod{\eta_8 \cdot 2^{-4}},$$

而

$$\left(\frac{3U_n}{\eta_8 \cdot 2^{-4}}\right) = \left(\frac{\pm 3 \cdot 41}{97}\right) = \left(\frac{\pm 3 \cdot 153}{97}\right) = -1。$$

4） $n \equiv 22 \pmod{24}$ 时，（1）不成立。

这时可设$n = -2 + 3 \cdot 2^t + 6 \cdot 2^t \cdot r$，$r \geqslant 0$，$t \geqslant 3$，由（8）式得

$$U_n \equiv \pm U_{-2+3\cdot 2^t} \pmod{\eta_{6\cdot 2^t} \cdot 2^{-3\cdot 2^t}}。$$

因为

$$U_{-2+3\cdot 2^t} = \frac{\xi_{6\cdot 2^t - 3}}{2^{3\cdot 2^t - 2}} = \frac{\eta_{6\cdot 2^t}\xi_{-3} + \eta_{-3}\xi_{6\cdot 2^t}}{2^{3\cdot 2^t - 2}}$$

$$\equiv 5 \cdot \frac{\xi_{6\cdot 2^t}}{2^{3\cdot 2^t}} \pmod{\eta_{6\cdot 2^t} \cdot 2^{-3\cdot 2^t}}$$

故这种情形将在下面的5)中得到处理。

5） $n \equiv 1 \pmod{24}$ 且$n \neq 1$时，（1）不成立。

此时不妨设$n = 1 + 3 \cdot 2^t + 6 \cdot 2^t \cdot r$，$r \geqslant 0$，$t \geqslant 3$，于是有

$$U_n \equiv \pm U_{1+3\cdot 2^t} \pmod{\eta_{6\cdot 2^t} \cdot 2^{-3\cdot 2^t}}。$$

因为

$$U_{1+3\cdot 2^t} = \frac{\xi_{6\cdot 2^t + 3}}{2^{3\cdot 2^t}} = \frac{\eta_{6\cdot 2^t}\xi_3 + \eta_3\xi_{6\cdot 2^t}}{2^{3\cdot 2^t + 1}}$$

$$\equiv 5 \cdot \frac{\xi_{6\cdot 2^t}}{2^{3\cdot 2^t}} \pmod{\eta_{6\cdot 2^t} \cdot 2^{-3\cdot 2^t}},$$

而令

$$\theta_t = \frac{\xi_{2^t}}{2^{2^{t-1}}}, \quad \phi_t = \frac{\eta_{2^t}}{2^{2^{t-1}}},$$

可得

$$\phi_{t+1} = 2\phi_t^2 - 1 = 6\theta_t^2 + 1 = \phi_t^2 + 3\theta_t^2,$$

$$\theta_{t+1} = 2\theta_t\phi_t,$$

$$\phi_t^2 = 3\theta_t^2 + 1,$$

$$\frac{\eta_{6\cdot 2^t}}{2^{3\cdot 2^t}}=\phi_{t+1}\ (4\phi_{t+1}^2-3),$$

$$\frac{\xi_{6\cdot 2^t}}{2^{3\cdot 2^t}}=\theta_{t+1}\ (4\phi_{t+1}^2-1)\text{。}$$

故

$$U_{1+3\cdot 2^t}\equiv\pm 5\theta_{t+1}\ (4\phi_{t+1}^2-1)\ (\bmod \phi_{t+1}(4\phi_{t+1}^2-3)),$$

即有

$$U_{1+3\cdot 2^t}\equiv\mp 5\theta_{t+1}\ (\bmod\ \phi_{t+1})\text{。}$$

由于 $\phi_1=\frac{\eta_2}{2}=2$，$\phi_2=2\phi_1^2-1=7$，故在 $t\geqslant 3$时用归纳法可推出

$$\phi_t\equiv 1\ (\bmod 3),\ \phi_t\equiv 2\ (\bmod 5),\ \phi_t\equiv 1\ (\bmod 8)\text{。}$$

于是，如果（1）有解，必有

$$1=\left(\frac{3U_{1+3\cdot 2^t}}{\phi_{t+1}}\right)=\left(\frac{3}{\phi_{t+1}}\right)\left(\frac{\mp 5\theta_{t+1}}{\phi_{t+1}}\right)$$

$$=\left(\frac{3}{\phi_{t+1}}\right)\left(\frac{5}{\phi_{t+1}}\right)\left(\frac{\theta_{t+1}}{\phi_{t+1}}\right)$$

$$=\left(\frac{\phi_{t+1}}{3}\right)\left(\frac{\phi_{t+1}}{5}\right)\left(\frac{2\theta_t\phi_t}{\phi_t^2+3\theta_t^2}\right)$$

$$=\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)\left(\frac{3}{\phi_t}\right)=-1,$$

这是一个矛盾。

综合1)～5)可知，如果（1）成立，则 $n=1$，$y=1$，推出丢番图方程$x^2-27y^4=-2$ 仅有正整数解 $x=5$，$y=1$ 证毕。

利用以上类似的方法，还可证明：丢番图方程

$$x(x+1)(x+2)(x+3)=3y(y+1)(y+2)(y+3) \tag{10}$$

仅有正整数解 $x=3$，$y=2$和$x=7$。$y=5$。这是因为，如果令$X=2x+3$，$Y=2y+3$，则方程（10）化为

$$\left(\frac{X^2-5}{4}\right)^2-3\left(\frac{Y^2-5}{4}\right)^2=-2。$$

例 2 丢番图方程

$$(x^2-2y^2)^2-2y^4=-1 \tag{11}$$

仅有正整数解$x=1$，$y=1$。

证 由Pell方程的结果，（11）给出

$$|x^2-2y^2|+y^2\sqrt{2}=\delta^{2n+1},\ n\geqslant 0, \tag{12}$$

其中$\delta=1+\sqrt{2}$为Pell方程$x^2-2y^2=-1$的基本解。令$\overline{\delta}=1-\sqrt{2}$，则（12）得出

$$|x^2-2y^2|=\frac{\delta^{2n+1}+\overline{\delta}^{2n+1}}{2},\ y^2=\frac{\delta^{2n+1}-\overline{\delta}^{2n+1}}{2\sqrt{2}}, \tag{13}$$

令

$$x_r=\frac{\delta^r+\overline{\delta}^r}{2},\quad y_r=\frac{\delta^r-\overline{\delta}^r}{2\sqrt{2}},\ r>0.$$

则有如下的递推序列

$$x_{r+1}=2x_r+x_{r-1},\ x_0=1,\ x_1=1。 \tag{14}$$

现由（13）知

$$x^2-2y^2=\varepsilon x_{2n+1},\ y^2=y_{2n+1},\ \varepsilon=\pm 1,$$

由此推出

$$x^2=\varepsilon x_{2n+1}+2y_{2n+1},\ \varepsilon=\pm 1。 \tag{15}$$

当$\varepsilon=1$时，由于$x_{r+1}=x_r+2y_r$知

$$x^2=x_{2n+1}+2y_{2n+1}=x_{2n+2},$$

故

$$x^2=x_{2(n+1)}=\frac{\delta^{2(n+1)}+\overline{\delta}^{2(n+1)}}{2}$$

$$=4\left(\frac{\delta^{n+1}-\overline{\delta}^{n+1}}{2\sqrt{2}}\right)^2+(-1)^{n+1},$$

此给出 $x=1$，从而 $y=1$。

当$\varepsilon=-1$时，由于

$$x_{-r}=(-1)^r x_r,\quad y_{-r}=(-1)^{r-1}y_r,$$

故（15）给出

$$x^2=-x_{2n+1}+2y_{2n+1}=x_{2(-n)-1}+2y_{2(-n)-1}=x_{2l},$$

其中 $l=-n$。与前类似仍得$x=1$。证毕。

丢番图方程$x^2+1=2y^4$的初等解法是一个困难的问题，例 2 只解决这个方程的一个特殊情形。我们看到，如果方程 $x^2+1=2y^4$ 有解，则有

$$y^2=y_{2n+1},\tag{16}$$

而 y_{2n+1}适合递推序列

$$y_{r+1}=2y_r+y_{r-1},\quad y_0=0,\quad y_1=1。$$

对这个递推序列取模16得出：

$$\underbrace{0,1,2,5,12,13,6,9,8,9,10,13,4,5,14,1,}\ \underbrace{0,1,}\cdots,\tag{17}$$

由此看出，（16）成立可推出$n\equiv0$，3，4，7（mod 8），即 $n\equiv0$，3（mod 4）。我们相信，利用递推序列的方法，可以彻底解决方程（16），但将需要一些特殊的技巧。

由上面的例题可以看出，许多利用递推序列法解决的丢番图方程，都可以用Pell方程的结果将其转化为递推序列。然而，还有一些丢番图方程是利用代数数论和其他方法后才转化为递推序列的。这在第三章将作部分介绍，更多的则放在以后的各章内介绍。

现在我们来讨论一些递推序列表平方数等的问题。

对于Fibonacci 序列

$$F_{n+2}=F_{n+1}+F_n,\quad F_0=0,\quad F_1=1,\tag{18}$$

容易知道

$$F_n=\frac{\alpha^n-\bar{\alpha}^n}{\sqrt{5}},\quad n\geqslant0,$$

其中 $\alpha=\frac{1+\sqrt{5}}{2}$，$\bar{\alpha}=\frac{1-\sqrt{5}}{2}$。与（18）相伴还有序列（也称Fibonacci 序列）

$$Q_{n+2}=Q_{n+1}+Q_n,\quad Q_0=2,\quad Q_1=1, \tag{19}$$

其中

$$Q_n=\alpha^n+\bar{\alpha}^n,\quad n\geqslant 0。$$

例 3 $F_n=x^2\Longleftrightarrow n=0$，1，2；$F_n=2x^2\Longleftrightarrow n=0$，3，6；$Q_n=x^2\Longleftrightarrow n=1$，3；$Q_n=2x^2\Longleftrightarrow n=0$，6。

证 先研究 F_n 和 Q_n 的一些数论性质。

1） 对 Q_n 取模 4 得到一个周期为6的序列

$$\underbrace{2,\ 1,\ 3,\ 0,\ 3,\ 3,}\ \underbrace{2,\ 1,\ \cdots\cdots},$$

故仅当$n\equiv 0$，3（mod6），即$n\equiv 0(\bmod 3)$时 $Q_n\equiv 0(\bmod 2)$；当$n\equiv\pm 2$（mod 6）时，$Q_n\equiv 3$（mod 4）。对Q_n取模 3 可以得出一个周期为8的序列

$$\underbrace{2,\ 1,\ 0,\ 1,\ 1,\ 2,\ 0,\ 2,}\ \underbrace{2,\ 1,\ \cdots\cdots},$$

故仅当$n\equiv 2$，6（mod8），即$n\equiv 2(\bmod 4)$时$Q_n\equiv 0$（mod3）。

2） F_n和 Q_n满足

$$Q_n^2-5F_n^2=4(-1)^n。$$

由1)知，当$n\equiv 0$（mod3）时，$Q_n\equiv 0$（mod2），故上式给出 $F_n\equiv 0$（mod2）；当$n\not\equiv 0$（mod3）时，$Q_n\not\equiv 0$（mod2），故 $F_n\not\equiv 0$（mod2）。于是

$$(F_n,\ Q_n)=1\Longleftrightarrow n\not\equiv 0\ (\bmod 3),$$

$$(F_n,\ Q_n)=2\Longleftrightarrow n\equiv 0\ (\bmod 3)。$$

3)直接验证如下的关系：

$$2F_{m+n}=F_mQ_n+F_nQ_m,$$

$$2Q_{m+n}=5F_mF_n+Q_mQ_n,$$

$$Q_{2m}=Q_m^2+2(-1)^{m-1},$$

$$F_{2m}=F_mQ_m。$$

4)　设$k\equiv\pm2$ (mod6)，则有

$$Q_{n+2kt}\equiv(-1)^tQ_n\pmod{Q_k},\quad t>0,$$

$$F_{n+2kt}\equiv(-1)^tF_n\pmod{Q_k},\quad t>0。$$

这两式的证明与例1中的递推序列类似。

下面我们只证明 $Q_n=x^2\Longleftrightarrow n=1$，3，其它的情形由1)～4)均不难得到，作为习题由读者完成。

设$Q_n=x^2$，若$n\equiv0$ (mod2)，设$n=2m$，则有$Q_{2m}=Q_m^2+2(-1)^{m-1}=x^2$，而这显然不成立。

现在考虑$n\equiv1$ (mod2)。设$n\equiv c$ (mod4)，$c=1$ 或 3。

如果$n>3$，可设$n=c+2\cdot3^rk$，$r\geqslant0$且$k\equiv\pm2$(mod6)。于是，由4)知

$$Q_n=Q_{c+2\cdot3^rk}\equiv(-1)^{3^r}Q_c=-Q_c\pmod{Q_k}。$$

由于 (19) 给出$Q_1=1$，$Q_3=4$，故由$Q_k\equiv3$ (mod 4) 知

$$\left(\frac{Q_n}{Q_k}\right)=\left(\frac{-Q_c}{Q_k}\right)=-1,$$

这就给出 $Q_n=x^2$ 在 $n>3$ 时不成立。于是 $n=1$，3。又知$Q_1=1$，$Q_3=4$均是平方数，故知$Q_n=x^2\Longleftrightarrow n=1,3$。证毕。

一方面，有一些丢番图方程可以化为递推序列来解；另一方面，丢番图方程的解也可以用来研究递推序列。例如，丢番图方程$x^4-Dy^2=1$的结果可在递推序列

$$x_{n+2}=2ax_{n+1}-x_n,\quad x_0=1,\quad x_1=a>1 \tag{20}$$

中得到应用（递推序列 (20) 称为Pell序列）。设 $a^2-1=Db^2$，$D>0$无平方因子，则 (20) 的解是

$$x_n=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2},\quad \varepsilon=a+b\sqrt{D},\quad \bar{\varepsilon}=a-b\sqrt{D}$$

如果方程$x^4-Dy^2=1$有解，则有

$$x^2=x_n。$$

举一个例子。我们在§6的例2中证明了丢番图方程 $x^4-6y^2=1$仅有正整数解$x=7$，$y=20$。由此可推出Pell序列

$$x_{n+2}=10x_{n+1}-x_n,\quad x_0=1,\quad x_1=5$$

中，除开$x_0=1$，$x_2=49$外，无其它的平方数。

还有一些递推序列是比较复杂的。为了说明这个问题，我们一般地看一下递推序列

$$x_{n+2}=Lx_{n+1}+Mx_n,\quad x_0=a,\quad x_1=b, \tag{21}$$

这里L，M，a和b均是给定的整数。我们知道（21）的解是

$$x_n=A_1\alpha^n+A_2\bar{\alpha}^n,\quad n\geqslant 0,$$

其中 α，$\bar{\alpha}$ 是方程 $z^2-Lz-M=0$的两个根，而A_1，A_2由$x_0=a$，$x_1=b$ 定出。对一元二次方程 $z^2-Lz-M=0$，其根的判别式为$\triangle=L^2+4M$，如果$\triangle\geqslant 0$，则序列（21）的各项容易判断正负，这时可用上述方法或二次剩余法（§5）研究x_n是否是 x^2或 nx^2。但是，如果$\triangle<0$，则序列（21）中的各项是正是负也难以确定。这时，即使求出 $x_n=\pm c$(c为给定的常数）的全部解 n 也非常困难。我们这里给出一个处理方法，它是W.Johnson[10]用来解决著名的 Ramanujan方程$x^2+7=2^n$ 时获得的。这个方法在代数数论方法中也常用到。

例 4 对于递推序列

$$x_{n+2}=x_{n+1}-2x_n,\quad x_1=x_2=1, \tag{22}$$

我们有$x_n=\pm 1$ $(n\geqslant 1)$ $\Longleftrightarrow n=1,\ 2,\ 3,\ 5$和 13。

证 由（22）可知

$$x_n=\frac{\omega^n-\bar{\omega}^n}{\omega-\bar{\omega}},\quad n\geqslant 1, \tag{23}$$

这里$\omega=\dfrac{1+\sqrt{-7}}{2}$，$\overline{\omega}=\dfrac{1-\sqrt{-7}}{2}$，$\omega+\overline{\omega}=1$和$\omega\overline{\omega}=2$。

令 y_n 适合

$$y_n+x_n\omega=\omega^n, \tag{24}$$

则由（23）代入（24）知$y_n=-2x_{n-1}$，因此 x_n，y_n 均是整数。由于

$$\begin{aligned}y_{n+1}+x_{n+1}\omega=\omega^{n+1}&=(y_n+x_n\omega)\omega\\&=y_n\omega+x_n\omega(1-\overline{\omega})\\&=(y_n+x_n)\omega-2x_n,\end{aligned}$$

故

$$y_{n+1}=-2x_n,\quad x_{n+1}=y_n+x_n。\tag{25}$$

于是

$$\begin{aligned}\omega^n=y_n+x_n\omega&=(x_{n+1}-x_n)+x_n\omega\\&=x_{n+1}-x_n\overline{\omega},\end{aligned}$$

故

$$\omega^{nk}=x_{n+1}^k+\sum_{j=1}^{k}(-1)^j\binom{k}{j}x_{n+1}^{k-j}x_n^j\overline{\omega}^j,\quad k\geqslant1,$$

由此两端乘以ω，得

$$\begin{aligned}\omega^{nk+1}=&x_{n+1}^k\omega-2kx_{n+1}^{k-1}x_n\\&+2x_n^2\sum_{j=2}^{k}(-1)^j\binom{k}{j}x_{n+1}^{k-j}x_n^{j-2}\overline{\omega}^{j-1},\quad k\geqslant2。\end{aligned}\tag{26}$$

因为由（23）及（25）知

$$\begin{aligned}\overline{\omega}^n&=\omega^n-(\omega-\overline{\omega})x_n\\&=y_n+x_n\omega-(2\omega-1)x_n\\&=y_n+x_n-x_n\omega\\&=x_{n+1}-x_n\omega,\end{aligned}$$

故（26）给出

$$y_{nk+1}+x_{nk+1}\omega=x_{n+1}^{k}\omega-2kx_{n+1}^{k-1}x_{n}$$
$$+2x_{n}^{2}\sum_{j=2}^{k}(-1)^{j}\binom{k}{j}x_{n+1}^{k-j}x_{n}^{j-2}\cdot$$
$$\cdot(x_{j}-x_{j-1}\omega),\quad k\geqslant 2,$$

由此即得

$$x_{nk+1}=x_{n+1}^{k}-2x_{n}^{2}\sum_{j=2}^{k}(-1)^{j}\binom{k}{j}x_{n+1}^{k-j}x_{n}^{j-2}x_{j-1},\quad k\geqslant 2。\tag{27}$$

现在对（22）所示的递推序列 x_n 取模16得出周期序列

1，1，15，13，15，5，7，13，15，…，

故 $x_n=1\Longleftrightarrow n=1,\ 2$；并且，如果 $x_n=-1$，则 $n=3$ 或 $n=4k+1$，$k\geqslant 1$。$n=3$时由（22)知$x_3=-1$。假设 $x_{4k+1}=-1$，$k\geqslant 1$，如果 $k=1$，易知 $x_5=-1$；如果 $k\geqslant 2$，则由（27）知

$$-1=x_{4k+1}=x_{5}^{k}-2x_{4}^{2}\sum_{j=2}^{k}(-1)^{j}\binom{k}{j}x_{5}^{k-j}x_{4}^{j-2}x_{j-1},\tag{28}$$

因为$x_4=-3$（从(22)直接推得），$x_5=-1$，故对（28）取模 3 得$-1\equiv(-1)^{k}\pmod 3$，此给出 $2\nmid k$，$x_5^k=-1$，故（28）即为

$$\sum_{j=2}^{k}(-1)^{j}\binom{k}{j}3^{j-2}x_{j-1}=0,\quad k>1,\quad 2\nmid k。\tag{29}$$

由于$k=3$时（29）式成立，这时 $x_{13}=-1$，故考虑 $k\geqslant 5$。在（29）中除去$k(k-1)$，则得

$$\frac{1}{2}-\frac{k-2}{2}+\sum_{j=4}^{k}(-1)^{j}\binom{k-2}{j-2}\frac{3^{j-2}}{j(j-1)}x_{j-1}=0。\tag{30}$$

在$j\geqslant 4$时，把$\frac{3^{j-2}}{j(j-1)}$化为既约分数时，分子被 3 整除。故（30）式推出$3\mid k$。

把k换为$3k$，$2\nmid k$。假设 $x_{12k+1}=-1$，除去 $k=1$，$x_{13}=-1$外可设$k\geqslant 3$，于是从（27）可得

$$-1=x_{12k+1}=x_{13}^k-2x_{12}^2\sum_{j=2}^{k}(-1)^j\binom{k}{j}x_{13}^{k-j}x_{12}^{j-2}x_{j-1},$$

由$x_{13}=-1$，$x_{12}=45$知，上式即为

$$\sum_{j=2}^{k}\binom{k}{j}45^{j-2}x_{j-1}=0\ , \qquad (31)$$

两端除去$k(k-1)$，则得

$$\frac{1}{2}+\sum_{j=3}^{k}\binom{k-2}{j-2}\frac{45^{j-2}}{j(j-1)}x_{j-1}=0,\quad k\geqslant 3。\qquad (32)$$

但在$j\geqslant 3$时把$\frac{45^{j-2}}{j(j-1)}$化为既约分数时，分子被5整除，故（32）式推出$5|1$的矛盾结果。这就证明了 $x_n=\pm 1(n\geqslant 1)$ $\Leftarrow\Rightarrow n=1$，2，3，5和13。证毕。

例4 的方法可以用来处理更多的丢番图问题。例如，可用来处理推广的 Ramanujan 方程

$$x^2+7^y=2^z$$

和

$$x^2+D=p^z,\quad p\nmid D>0,\quad p\ 奇素数，等等。$$

在证明例 4 中，对（29）和（31）式的处理，实际是比较素数幂法的一种变形。例如对（29）式，如果$3\nmid k$，设$3^u\|k-1$，则u是方程（29）左端的最高方幂，与右端0矛盾。对（31）式，如果设$5^u\|k(k-1)$，则左端含5的最高方幂为u，仍与右端为0矛盾。

利用递推序列法可以解决一些比较困难的问题，尽管处理的方法常常需要一些特殊的技巧，且证明过程也比较麻烦，但它仍不失为一个得力的初等方法。

习　　题

1. 证明丢番图方程$x^2+2=3^n$仅有正整数解 $x=1$，$n=1$和 $x=5$，$n=3$。

2. 设p是素数，$e\geqslant 0$，则丢番图方程

$$(2^e py^2-1)^2+1=2z^2$$

仅有正整数解$z=1$，5和 $p=2$。

3. 证明丢番图方程

$$x(x+1)(x+2)(x+3)=2y(y+1)(y+2)(y+3)$$

仅有正整数解 $x=5$，$y=4$。

4. 证明丢番图方程 $3x^4-2y^2=1$ 仅有正整数解 $x=y=1$和 $x=3$，$y=11$。

5. 证明丢番图方程 $x(x+1)(2x+1)=6y^2$ 仅有正整数解 $x=1$，$y=1$和$x=24$，$y=70$。

6. 证明丢番图方程 $(2y^2-3)^2=x^2(3x^2-2)$ 仅有正整数解 $x=y=1$和$x=y=3$。

7. 证明丢番图方程$x^2-3y^4=1$仅有正整数解 $x=2$，$y=1$和 $x=7$，$y=2$。

§8　其他的一些初等方法

I．不等式法

在前面我们已经介绍了解丢番图方程的七种初等方法，它们都是用来制造等式不成立的基本工具。这里等式不成立即“不等”，与通常意义下的“不等”是有一定区别的。例如，在比较素数幂法中，由于等式$f=g$两端所含p的最高方幂不等，从而推出$f\neq g$。因此对 $f-g$，我们没有得出一

个固定的符号。作为证明丢番图方程无解的一个方法（或思路），判断何时$f-g>0$或$f-g<0$是必需的。例如，柯召[11]利用这种方法(我们称为不等式法）证明了Catalan方程

$$x^q=y^p+1,\quad p>2\text{和}q\text{ 均是素数} \tag{1}$$

有正整数解的充要条件是

$$1)\quad y+1=p^{s q-1}x_1^q,\quad \frac{y^p+1}{y+1}=p x_2^q,\quad x=p^s x_1 x_2,$$

这里x_1，x_2和s都是正整数，$(x_1, x_2)=1$且$p\nmid x_1 x_2$。 或

$$2)\quad x-1=q^{t p-1}y_1^p,\quad \frac{x^q-1}{x-1}=q y_2^p,\quad y=q^t y_1 y_2,$$

这里y_1，y_2和t都是正整数，$(y_1, y_2)=1$且$q\nmid y_1 y_2$。

下面我们举两个例子以说明不等式法的使用。

例 1 丢番图方程

$$\sum_{j=1}^{x} j^y=\left(\frac{x(x+1)}{2}\right)^y \tag{2}$$

除开$x=1$ 或 $y=1$外，无其他的正整数解。

证 除开$x=1$或$y=1$是（2）的解外，可设$x>1$，$y>1$我们首先来证明：对于任给k个正 数x_1，x_2，…，x_k，在$k>1$，$n>1$时有

$$x_1^n+\cdots+x_k^n<(x_1+\cdots+x_k)^n。 \tag{3}$$

用归纳法。$k=2$时 由 $n>1$ 知，$(x_1+x_2)^n=x_1^n+\cdots+x_2^n>x_1^n+x_2^n$。设(3)成立，则有

$$x_1^n+\cdots+x_k^n+x_{k+1}^n<(x_1+\cdots+x_k)^n+x_{k+1}^n<$$
$$(x_1+\cdots+x_k+x_{k+1})^n,$$

这就证明了（3)。利用不等式（3)，注意到$1+2+\cdots+x=\frac{x(x+1)}{2}$立得$\sum_{j=1}^{x} j^y<\left(\frac{x(x+1)}{2}\right)^y$（当$x>1$，$y>1$）。这就

证明了例1。

例 2 丢番图方程

$$x^2-1=y^p, \quad p>3\text{是素数} \tag{4}$$

没有正整数解。

证 在§6的例3中我们已知，方程(4)有解时必有$2|y$，$p|x$。因为$2\nmid x$，$(x-1, x+1)=2$，故(4)给出

$$x+1=2^{p-1}y_1^p, \quad x-1=2y_2^p, \tag{5}$$

或

$$x+1=2y_2^p, \quad x-1=2^{p-1}y_1^p, \tag{6}$$

这里$y=2y_1y_2$，$2\nmid y_2$，且$(y_1, y_2)=1$。在(5)时，我们有$y_2^p=2^{p-2}y_1^p-1$，由此整理得

$$(y_2^2)^p+(2y_1)^p=(y_2^p+2)^2=\left(\frac{x+3}{2}\right)^2, \tag{7}$$

由于$p|x$，$p>3$，故$p\nmid\dfrac{x+3}{2}$。因此$\left(y_2^2+2y_1, \dfrac{(y_2^2)^p+(2y_1)^p}{y_2^2+2y_1}\right)=1$，由(7)式得出

$$y_2^2+2y_1=h^2, \tag{8}$$

由此整理得

$$(hy_2)^2+y_1^2=(y_2^2+y_1)^2。 \tag{9}$$

因为$(y_1, y_2)=1$，所以$(hy_2, y_1)=1$。注意到$2\nmid y_2$，由(8)推出$2\nmid h$，$2|y_1$，所以由方程$x^2+y^2=z^2$，$(x, y)=1$的结果（参见§2的例1）知，(9)给出

$$hy_2=a^2-b^2, \quad y_1=2ab, \quad y_2^2+y_1=a^2+b^2 \quad (a>b>0),$$

于是知$(a-b)^2=(y_2^2+y_1)-y_1=y_2^2$，得$y_2=a-b$。由$y_1-y_2=2ab-(a-b)=a(2b-1)+b>0$得$y_1>y_2$。但由(5)知$y_2^p=2^{p-2}y_1^p-1>y_1^p$ $(p>3)$，这不可能。

对于（6）式，消去x可得

$$(y_2^2)^p-(2y_1)^p=(y_2^p-2)^2=\left(\frac{x-3}{2}\right)^2,$$

由此知

$$y_2^2-2y_1=h^2,\quad h\left|\frac{x-3}{2}\right.。$$

于是 $(hy_2)^2+y_1^2=(y_2^2-y_1)^2$，此给出（注意，上式给出 $y_2^2-y_1>0$）

$hy_2=a^2-b^2$，$y_1=2ab$，$y_2^2-y_1=a^2+b^2$ $(a>b>0)$，由此求出 $y_2=a+b$，故 $y_1-y_2=2ab-(a+b)=(a-1)(b-1)+(ab-1)>0$，而由$y_2^p=2^{p-2}y_1^p+1>y_1^p$知，仍不可能。证毕。

由上面的例题可知，不等式法就是利用各种方法把问题展开，然后出其不意地比较某两个数（或式子）的大小。

Ⅱ．利用整函数的某些性质解丢番图方程

整函数是指这样的函数：变元取整数时，函数值也是整数。例如，整系数多项式为整函数，$\binom{x}{r}$也是整函数，这里

$$\binom{x}{r}=\frac{x(x-1)\cdots(x-r+1)}{r!}。$$

现在我们给出函数 $A(n)=\dfrac{x^n-y^n}{x-y}$，$(x,y)=1$ 的一些结果。

例 3 设p是奇素数，则$A(p)$至少含有一个$2mp+1$形的素因子。

证 显然$2\nmid A(p)$，设$q\mid A(p)$，由 $(x-y,A(p))=1$ 或p知，除$q=p$外$q\nmid x-y$。现在我们证明，如果 $q=p$，则

在$A(p)$中除p外，至少含有一个另外的素因子。这是因为

$$A(p)=x^{p-1}+x^{p-2}y+\cdots+xy^{p-2}+y^{p-1}>p。$$

于是可设$q\nmid x-y$，$q\mid A(p)$。我们来证明q是$2mp+1$形的素数。显然$q\nmid xy$，取$z\equiv xy^{q-2}\pmod{q}$，则

$$z^p-1\equiv(xy^{q-2})^p-(y^{q-1})^p\equiv(y^p)^{q-2}(x^p-y^p)\equiv0\pmod{q}$$

设g是模q的一个元根，令$z\equiv g^l\pmod{q}$，则有

$$z^p-1\equiv g^{pl}-1\equiv0\pmod{q},$$

因此$(q-1)\mid pl$。如果$p\nmid q-1$，则$(q-1)\mid l$，设$l=(q-1)l_1$，则$z\equiv g^l\equiv g^{(q-1)l_1}\equiv1\pmod{q}$ 但 $z-1\equiv xy^{q-2}-y^{q-1}\equiv y^{q-2}(x-y)\not\equiv0\pmod{q}$，矛盾。于是$p\mid q-1$，从而$q$是$2mp+1$形的素数。证毕。

利用例3，结合二次剩余法，可以证明§5的例5。现在给出例3的一个推论。

例 4 设D不含$2mp+1$形的素因子，则丢番图方程

$$x^p-y^p=D,\ (x,\ y)=1 \tag{10}$$

无正整数解。

证 假设(10)有正整数解，则有

$$(x-y)\left(\frac{x^p-y^p}{x-y}\right)=(x-y)A(p)=D。$$

由例3知，$A(p)$至少含有一个$2mp+1$形素因子q，故上式给出$q\mid D$，这与D的假设矛盾。证毕。

在1904年，Birkhoff和Vandiver曾证明一个推广例3的结果，即有：设$n>6$，则$A(n)$至少含有一个$mn+1$形的素因子。后来，在1913年Carmichael把$A(n)$换为Lucas序列

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}(\alpha,\beta\text{为}x^2-Rx+S=0\text{的两个根},(R,S)=1)$$

也得到了类似的结果。1974年，Achinzel对一般的代数整

数也得到了类似的结果。这些结果，正如例 3 在解丢番图方程中的应用（例4）一样，都可以用来解相应的丢番图方程。

有趣的是，1981年 M. Newman[12] 利用一个整函数的不可约性，给出了丢番图方程

$$x^{\frac{1}{m}}+y^{\frac{1}{n}}=z^{\frac{1}{r}}，m，n\text{和}r\text{均是正整数} \tag{11}$$

的全部正整数解。

例 5 设 $a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$s\geqslant1$，$\alpha_i\neq0$且$p_i$是不同的素数（$i=1,\cdots,s$），则

$$f(x)=x^n-a \tag{12}$$

在有理数域上不可约的充要条件是 $(n,v(a))=1$。这里 $v(a)=(\alpha_1,\cdots,\alpha_s)$。

证 由于$v(a)=(\alpha_1,\cdots,\alpha_s)$，故可写$a=b^{v(a)}$。如果$f(x)$在$Q$上不可约，设$d=(n,v(a))$，$n=dn_1$，$v(a)=dv_1$，则有

$$f(x)=x^n-b^{v(a)}=x^{dn_1}-b^{dv_1}$$

$$=(x^{n_1}-b^{v_1})\frac{(x^{n_1})^d-(b^{v_1})^d}{x^{n_1}-b^{v_1}}。$$

此在$d>1$时与$f(x)$在Q上不可约矛盾。故$d=1$。

现设$d=1$，如果$f(x)$可约，可设

$$f(x)=f_1(x)f_2(x),$$

其中 $f_1(x)$ 为首项系数等于1的k（$1\leqslant k\leqslant n$）次有理系数多项式。设η是n次单位原根，则

$$x^n-a=\prod_{i=1}^{n}(x-\eta^ia^{\frac{1}{n}})。$$

不妨设

$$f_1(x)=\prod_{j=1}^{k}(x-\eta^{i_j}a^{\frac{1}{n}}),\quad 1\leqslant i_1\leqslant i_2<\cdots<i_k<n,$$

因为 $\prod_{j=1}^{k}(\eta^{i_j}a^{\frac{1}{n}})$是有理数，故$\pm a^{\frac{k}{n}}$为有理数，即

$$a^{\frac{k}{n}}=\prod_{i=1}^{s}p_i^{\alpha_i\frac{k}{n}}\in Q,$$

所以 $\alpha_i\cdot\frac{k}{n}\equiv 0\ (\bmod 1)\ (i=1,\ \cdots,\ s)$。因此$v(a)=(\alpha_1,\ \cdots,\ \alpha_s)=\sum_{i=1}^{s}t_i\alpha_i$，故有$v(a)\cdot\frac{k}{n}\equiv 0\ (\bmod 1)$，由$d=(n,\ v(a))=1$知$\frac{k}{n}\equiv 0(\bmod 1)$。此给出$k\geqslant n$，与$k<n$矛盾。证毕。

利用例5，M.Newman 证明了方程（11）的全部正整数解可由

$$x=t^{m/d}a^n,\quad y=t^{n/d}b^n,\quad z=t^{r/d}(a+b)^r$$

表出，这里 $(m,\ n,r)=d$，a,b,t是任意正整数且$(a,\ b)=1$。

应该指出，在1979年戴宗铎、冯绪宁和于坤瑞[13]曾用代数数论的方法给出了方程 $x^{\frac{1}{n}}+y^{\frac{1}{n}}=z^{\frac{1}{n}}(n>1)$ 的全部正整数解；同时，他们证明了方程

$$x^{\frac{m_1}{n_1}}+y^{\frac{m_2}{n_2}}=z^{\frac{m_3}{n_3}},\quad (m_i,\ n_i)=1\text{且}m_i>0,\ n_i>0\quad (i=1,\ 2,\ 3)$$

有正整数解等价于方程

$$x^{d_1}+y^{d_2}=z^{d_3}$$

有正整数解，这里$d_1=(m_1,\ [m_2,m_3])$，$d_2=(m_2,[m_3,\ m_1])$和$d_3=(m_3,\ [m_1,\ m_2])$。

Ⅲ. 构造的方法

构造一个丢番图方程的解有很多用处。例如，P.Erdös 在三十年代末曾经猜想：丢番图方程

$$x^xy^y=z^z,\quad x>1,\quad y>1,\quad z>1 \tag{12}$$

无整数解。1940年柯召构造出方程（12）的无穷多组解，这

就否定了P.Erdös的这个猜想。1964年，柯召和孙琦[14]进一步构造出丢番图方程

$$\prod_{i=1}^{k} x_i^{x_i} = z^z,\ k\geqslant 2,\ x_i>1\ (i=1,\ \cdots,\ k)\quad (13)$$

的无穷多组解。即有

例 6 方程（13）有无穷多组整数解

$$x_1 = k^{k^n(k^{n+1}-2n-k)+2n}(k^n-1)^{2(k^n-1)},$$

$$x_2 = k^{k^n(k^{n+1}-2n-k)}(k^n-1)^{2(k^n-1)+2},$$

$$x_3 = \cdots = x_k = k^{k^n(k^{n+1}-2n-k)+n}(k^n-1)^{2(k^n-1)+1},$$

$$z = k^{k^n(k^{n+1}-2n-k)+n+1}(k^n-1)^{2(k^n-1)+1},$$

其中$k=2$时，$n>1$；$k\geqslant 3$时，$n>0$。

证 设 $(x_1,\ \cdots,\ x_k,\ z)=d$，令

$$x_i = dt_i,\ z = du,\ i=1,\ \cdots,\ k,$$

代入方程（13）得

$$d^{\sum_{i=1}^{k} t_i - u}\prod_{i=1}^{k} t_i^{t_i} = u^u。\quad (14)$$

如果能找到满足

$$\sum_{i=1}^{k} t_i - u = 1,\quad \prod_{i=1}^{k} t_i^{t_i} \Big| u^u \quad (15)$$

的 $t_i(i=1,\ \cdots,\ k)$ 和u，则由（14）式解出d，给出方程（13）的解。为此，令

$$t_1 = k^{2n},\ t_2 = (k^n-1)^2,\ t_3 = \cdots = t_k = (k^n-1)k^n,$$

$$u = k^{n+1}(k^n-1),$$

则

$$\sum_{i=1}^{k} t_i - u = k^{2n} + (k^n-1)^2 + (k-2)(k^n-1)k^n$$

$$- k^{n+1}(k^n-1) = 1。$$

又

$$\frac{u^n}{\prod_{i=1}^{k} t_i^{l_i}} =$$

$$\frac{k^{(n+1)k^{n+1}(k^n-1)} \cdot (k^n-1)^{k^{n+1}(k^n-1)}}{k^{2nk^{2n}}(k^n-1)^{(2k^n-1)^2}((k^n-1)^{(k^n-1)k^n} \cdot k^{n(k^n-1)k^n})^{k-2}}$$

$$= k^h (k^n-1)^l,$$

这里

$$\begin{aligned} h &= (n+1)k^{n+1}(k^n-1) - 2nk^{2n} - n(k-2)(k^n-1)k^n \\ &= k^n(k^{n+1} - k - 2n), \\ l &= k^{n+1}(k^n-1) - 2(k^n-1)^2 - (k-2)(k^n-1)k^n \\ &= 2(k^n-1)。\end{aligned}$$

显然在$k>2$，$n>0$或$k=2$，$n>1$时有$h>0$，$l>0$。故由(14)式给出

$$d = k^h(k^n-1)^l = k^{k^n(k^{n+1}-k-2n)} \cdot (k^n-1)^{2(k^n-1)},$$

于是知例6成立。

这个例子中，主要困难是构造满足（15）的 t_i（$i=1,\cdots,k$）和u。对于$k\geqslant 3$，还可构造满足(15)的另外一些解。但是，在$k=2$或$k=3$时，方程（13）是否存在 z 为奇数的解（简称奇数解）？我们猜想：$k=2$时不存在奇数解；而$k=3$时，一定存在奇数解。看来有希望用构造的方法，给出方程（13）在$k=3$时的一些奇数解。

对于丢番图方程

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{w}+\frac{1}{xyzw}=0, \qquad (16)$$

L.J.Mordell 曾经问，（16）的整数解怎样？最近，本书作者[15]给出了一个解答。首先根据正负号的讨论，可把（16）化为如下三个求正整数解的方程

$$\frac{1}{x}=\frac{1}{y_1}+\frac{1}{z_1}+\frac{1}{w_1}+\frac{1}{xy_1z_1w_1}, \tag{17}$$

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{xyz_1w_1}=\frac{1}{z_1}+\frac{1}{w_1}, \tag{18}$$

和

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{1}{w_1}+\frac{1}{xyzw_1}。 \tag{19}$$

然后，分别给出（17）～（19）的全部正整数解表达式。例如，方程（17）的全部正整数解可表为

$$x=n,\quad y_1=n+k,\quad z_1=n+\frac{n^2+t}{k},$$

$$w_1=\frac{1}{t}\left[n(n+k)\left(n+\frac{n^2+t}{k}\right)+1\right], \tag{20}$$

其中 n，k，t 为正整数，满足

1） $n^2+t\equiv 0 \pmod k$，

2） $n(n+k)\left(n+\frac{n^2+t}{k}\right)+1\equiv 0 \pmod t$

及

3） $(n,\ k)=(k,\ t)=(n,\ t)=1$。

由此看出，要给出方程（17）的正整数解，必须构造同时满足1)～3)的正整数n，k和 t 。显然在 $t=1$或 $k=1$ 时，满足1)～3)的正整数 n，k，t 是容易构造的。现在考虑 $k>1$ ，$t>1$ 。由1)～3)可证：

例 7 在$2|n$ 或 $2\nmid k$时，1)～3)给出 $k\equiv t\equiv 1 \pmod 4$ 且$\left(\frac{k}{t}\right)=1$。

证 在$2|n$时，由2)知 $2\nmid t$ ，从而1)给出$2\nmid k$。于是1)及

3)给出

$$\left(\frac{-t}{k}\right)=1。\tag{21}$$

现由2)及3)得

$$(n(n+k))^2+k\equiv 0 \pmod t,$$

故

$$\left(\frac{-k}{t}\right)=1。\tag{22}$$

由(21)和(22)得

$$1=\left(\frac{-t}{k}\right)\left(\frac{-k}{t}\right)=(-1)^{\frac{k-1}{2}+\frac{t-1}{2}}\left(\frac{t}{k}\right)\left(\frac{k}{t}\right)$$

$$=(-1)^{\frac{k-1}{2}+\frac{t-1}{2}+\frac{k-1}{2}\cdot\frac{t-1}{2}}$$

即有

$$\frac{k-1}{2}+\frac{t-1}{2}+\frac{k-1}{2}\cdot\frac{t-1}{2}\equiv 0 \pmod 2,$$

由此推出$k\equiv t\equiv 1 \pmod 4$，且由(22)知$\left(\frac{k}{t}\right)=1$。

在$2\nmid k$时，如果$2|n$，则与前同理可证；如果$2\nmid n$，则由于$2|(n+k)$，从2)知$2\nmid t$，仍与前同理可证。证毕。

例7 为我们构造(17)的解提供了一个依据。例如，可取$t=5$，$k=41$，由1)～2)解出$n\equiv 6, 88, 158 \pmod{205}$，以 $n=205n_1+6$为例代入方程(17)的解(20)中，得到

$x=205n_1+6$，$y_1=205n_1+47$，$z_1=1025n_1^2+265n_1+7$，

$w_1=8615125n_1^4+4454650n_1^3+692490n_1^2+30157n_1+395$。

应该注意到，丢番图方程(17)与丢番图方程

$$\frac{1}{x_1}+\cdots+\frac{1}{x_s}+\frac{1}{x_1\cdots x_s}=1,\ 1<x_1<\cdots<x_s \tag{23}$$

密切相关。例如，已知（23）在$s=t$时的一组解$x_1^{(0)}, \cdots, x_t^{(0)}$，令$A=x_1^{(0)}\cdots x_t^{(0)}$，则求$s>t$时的解可用如下的方法：把$x_1=x_1^{(0)}, \cdots, x_t=x_t^{(0)}$代入（23）得到

$$\frac{1}{x_{t+1}}+\cdots+\frac{1}{x_{t+l}}+\frac{1}{Ax_{t+1}\cdots x_{t+l}}=\frac{1}{A}, \qquad (24)$$

其中$t+l=s$。故可利用方程（17）的解来构造（24）的解。曹珍富等[16]利用电子计算机算出了方程（23）在$s=7$时的全部解，共26组。由这些解出发，可由（17）的解构造方程（23）在$s>7$时的解。

习　　题

1. 证明丢番图方程$x^n+1=y^{n+1}$没有$n\geq 2, (x, n+1)=1$的正整数解。

2. 证明丢番图方程

$$x^2=\frac{y^n+1}{y+1}, \quad 2\nmid n>1$$

无$|y|>2^{n-2}$的整数解。

3. 设$\Omega(s)$表方程（23）解的个数，证明：在$s\geq 4$时$0<\Omega(s)<\Omega(s+1)$。

4. 在$k>1$，$t\geq 1$时，构造方程（17）另外的一些解。

参 考 文 献

［1］柯召，四川大学学报(自然科学版)，1(1962)，1-6。

［2］Terjanian, G., C.R.Acad.Sci.Paris, 285 (1977), 973-975.

［3］曹珍富，东北数学，2（1986），219—227。

[4] Rotkiewicz, A., Acta Arith., 42 (1983), 163—187。

[5] 曹珍富，数学研究与评论， 2 (1987) ， 319—320, 318。

[6] Ljunggren, W., Skr. Norske Vid.-Akad. Oslo I, Mat.-Naturv. Kl. 1936, No. 12 。

[7] 曹珍富，自然杂志,6 (1985) ， 476—477。

[8] 曹珍富，西南师范大学学报（自然科学版），2 (1987) ， 16—19。

[9] Golomb, S. W. , Amer. Math. Monthly, 77 (1970) ， 848—852。

[10] Johnson, W., Amer. Math. Monthly, 94 (1987) ， 59—62。

[11] 柯召，四川大学学报(自然科学版)，2 (1963), 1—7。

[12] Newman, M., J.Number Theory,13(1981), 495—498。

[13] 戴宗铎、 冯绪宁、 于坤瑞， 科学通报， 10 (1979) ， 438—442。

[14] 柯召、孙琦，四川大学学报（自然科学版），2 (1964) ， 5—9。

[15] 曹珍富，数学杂志，3 (1987) ， 245—250。

[16] Cao, Z.F. (曹珍富) 等，J.Number Theory, 27 (1987) ， 206—211。

第三章　解丢番图方程的高等方法

我们知道，有些丢番图方程的求解是非常困难的（例如Fermat大定理(Fermat's last theorem)等）。人们为了解决这些丢番图方程，创立了许多数学方法，例如代数数论方法，p—adic方法和丢番图逼近方法等，这些方法大大丰富了数论的内容，同时也为我们求解更广泛地丢番图方程提供了有力的工具。

§1 代数数论方法（Ⅰ）

所谓代数数论方法，就是把所给丢番图方程放在代数数域中考虑，通过代数整环性质的讨论，使问题得到简化或展开。有些整环的唯一分解定理不成立，需要引进理想数的概念，把丢番图方程放到理想整环中去考虑。利用这种方法，可以把丢番图方程化为若干容易处理的或有熟知结果的方程。但是，仅用代数数论常常是不够的。一般情况下，是用代数数论的知识把方程展开或简化，综合运用其它方法（一般是初等方法）处理这些展开或简化后的方程。

为了便于我们说明这种方法，下面列出在解丢番图方程时经常用到的代数数论的一些基本概念和结果。以下常设Q和Z分别是有理数域和有理整环。

Ⅰ．如果θ是一个Q上系数为有理数的$n(n>0)$次不可约

多项式的根，则称θ为n次代数数；如果θ为一个首项系数为1，其余系数为有理整数（为了与下面的代数整数区别，称通常的整数为有理整数）的n次不可约多项式的根，则称θ为n次代数整数。

设θ是一个n次代数整数，则所有形如

$$\alpha = a_1 + a_2\theta + \cdots + a_n\theta^{n-1},\quad a_i \in Q\ (i = 1, \cdots, n) \qquad (1)$$

的数组成一个域，称为θ添加到Q上得到的n次代数数域，记为$Q(\theta)$。熟知，$Q(\theta)$中的整数构成一环，称为n次的代数整环$Z[\theta]$。若$\omega_1, \cdots, \omega^n \in Z[\theta]$，且$Z[\theta]$中任一整数$\omega$都可表为

$$\omega = a_1\omega_1 + \cdots + a_n\omega_n,\quad a_i \in Z\ (i = 1, \cdots n), \qquad (2)$$

则称$\omega_1, \cdots, \omega_n$是$Q(\theta)$的整底（如果把$Z[\theta]$和$Z$分别换为$Q(\theta)$和$Q$，则$\omega_1, \cdots, \omega_n$称为$Q(\theta)$的基底）。

记$\theta = \theta^{(1)}$，令$\theta^{(2)}, \cdots, \theta^{(n)}$为$\theta$所适合的$n$次不可约多项式的其他$n$—1个根，则称

$$\alpha^{(i)} = a_1 + a_2\theta^{(i)} + \cdots + a_n(\theta^{(i)})^{n-1} \quad (i = 2, \cdots, n)$$

为(1)式中α的共轭数。令$\alpha = \alpha^{(1)}$，则称

$$N(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)}$$

为α的范数(Norm)。如果$N(\alpha) = \pm 1$，则称α为$Q(\theta)$的单位数。Dirichlet对单位数曾证明了一个一般性的定理：假设$\theta^{(1)}$ $(=\theta)$，$\theta^{(2)}, \cdots, \theta^{(n)}$中有$r_1$个实数，$r_2$对共轭复数$(r_1 + 2r_2 = n)$，则在$Q(\theta)$的所有单位数中可取出$r = r_1 + r_2 - 1$个$\varepsilon_1, \cdots, \varepsilon_r$，使$Q(\theta)$中任一单位数$\varepsilon$可表为

$$\varepsilon = \rho\varepsilon_1^{t_1} \cdots \varepsilon_r^{t_r},\quad t_i \in Z (i = 1, \cdots, r),$$

其中ρ是$Q(\theta)$中的一个单位根。我们称Dirichlet定理中的$\varepsilon_1, \cdots, \varepsilon_r$为$Q(\theta)$的基本单位数。

Ⅱ. 二次域是经常用到的。设$D \neq 1$且$D \in Z$无平方因子，则$Q(\sqrt{D})$经过所有的二次域，故不失一般可设$Q(\sqrt{D})$为二

次域。

当$D\equiv 2$，$3(\mathrm{mod}4)$时，1，$\sqrt{D}$是$Q(\sqrt{D})$的一组整底；

当$D\equiv 1(\mathrm{mod}4)$时，1，$\frac{1+\sqrt{D}}{2}$是$Q(\sqrt{D})$的一组整底。

$Q(\sqrt{D})$的单位数与Pell方程有关。设$x+y\omega\left(\omega=\sqrt{D}\text{或}\frac{1+\sqrt{D}}{2}\right)$为$Q(\sqrt{D})$的单位数，$x+y\overline{\omega}$为$x+y\omega$的共轭数，则由

$$N(x+y\omega)=(x+y\omega)(x+y\overline{\omega})$$

$$=\begin{cases}(x+\frac{y}{2})^2-D\frac{y^2}{4}, & \text{当}D\equiv 1(\mathrm{mod}4)\\ x^2-Dy^2\quad, & \text{当}D\equiv 2,3(\mathrm{mod}4)\end{cases}$$

知，求出Pell方程

$$(2x+y)^2-Dy^2=\pm 4$$

和

$$x^2-Dy^2=\pm 1$$

的全部解可给出二次域$Q(\sqrt{D})$的全部单位数。我们有：

在$D<0$时，$Q(\sqrt{-1})$有四个单位数± 1，$\pm i$；$Q(\sqrt{-3})$有六个单位数± 1，$\pm\frac{1+\sqrt{-3}}{2}$，$\pm\frac{1-\sqrt{-3}}{2}$。除开这两种情形外，$Q(\sqrt{D})$都仅有单位数± 1。在$D>0$时，$Q(\sqrt{D})$中必存在基本单位数η，使得$Q(\sqrt{D})$的一切单位数皆可表为，

$$\pm\eta^n,\ n\in Z。$$

Ⅲ．与有理整环Z类似的，可在代数整环$Z[\theta]$上定义整

除、素数等概念，从而研究$Z[\theta]$上的唯一分解定理。

设α，$\beta\in Z[\theta]$，若$\gamma\in Z[\theta]$使$\alpha=\beta\gamma$，则称β整除α（也称β是α的因子），记为$\beta\mid\alpha$；否则称β不整除α，记为$\beta\nmid\alpha$。若α、β仅相差一个单位因子，则称α与β相结合。如果α除了单位数和与α相结合的整数外，不被$Z[\theta]$中其他整数整除，则α称为$Z[\theta]$或$Q(\theta)$中的素数。

很明显，任一非单位整数都可以写成若干素数的乘积（这个过程称为分解）。例如在$Z[\sqrt{-5}]$中，我们有

$$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5}),$$

而$2,3,1+\sqrt{-5}$和$1-\sqrt{-5}$都是$Z[\sqrt{-5}]$中的素数。由这个例子可以看出，代数整环$Z[\theta]$中的整数分解一般是不唯一的。但在许多丢番图方程的研究中，为了使问题得到展开，常常需要把所研究的问题放在整数唯一分解的整环中考虑，这就是当初Kummer引进理想数的原因。

设$\alpha_1,\cdots,\alpha_s\in Z[\theta]$，则由所有形如

$$\eta_1\alpha_1+\cdots+\eta_s\alpha_s,\quad \eta_i\in Z[\theta]\ (i=1,\cdots,s)$$

的数组成的集称为由$\alpha_1,\cdots,\alpha_s$生成的理想数，以$[\alpha_1,\cdots,\alpha_s]$表之。仅有一个代数整数$\alpha$生成的理想数$[\alpha]$称为主理想数。$[1]$和$[0]$分别称为单位理想数和零理想数。

$$设\ A=[\alpha_1,\cdots,\alpha_s],\ B=[\beta_1,\cdots,\beta_t],\ 定义$$

$$AB=[\alpha_1\beta_1,\cdots,\alpha_1\beta_t,\cdots,\alpha_s\beta_1,\cdots,\alpha_s\beta_t]。$$

如果理想数A除了单位理想数$[1]$和本身以外，不能分解出其他因子（或说不被其他理想数整除），则A称为素理想数。显然，任一理想数都可以分解为素理想数的乘积。可以证明，如果不计次序，理想数分解为素理想数的乘积是唯一的。

Ⅳ. 设$\alpha\in Z[\theta]$,理想数$A\mid[\alpha]$也记为$A\mid\alpha$或$\alpha\in A$。若$A\mid\alpha-\beta$, α, $\beta\in Z[\theta]$, 则称α, β对模A同余, 记为$\alpha\equiv\beta(\bmod A)$。利用同余关系, 可以将$Z(\theta)$中的所有数进行模$A$分类, 其类数记为$N(A)$, 称为理想数$A$的范数($N(A)$显然有限)。易知

1)设 $\alpha\in Z[\theta]$, 则$N([\alpha])=|N(\alpha)|$;

2) $N(AB)=N(A)N(B)$;

3)设 P为素理想数, $\alpha\in Z[\theta]$, 则

$$\alpha^{N(P)}\equiv\alpha(\bmod P)。$$

现在我们考虑有理素数p在二次域$Q(\sqrt{D})$中的分解。我们有: 设P, $\overline{P}$为素理想数, 则

1) $[p]=P\Leftrightarrow\left(\frac{\triangle}{P}\right)=-1$;

2) $[p]=P\overline{P}$, $P\neq\overline{P}$, $N(P)=N(\overline{P})=p$

$$\Leftrightarrow\left(\frac{\triangle}{p}\right)=1;$$

3) $[p]=P^2$, $N(P)=p\Leftrightarrow\left(\frac{\triangle}{p}\right)=0$ 。

这里

$$\triangle=\begin{cases}D, & 当D\equiv1(\bmod4)\\4D, & 当D\equiv2,3(\bmod4)\end{cases}$$

称为$Q(\sqrt{D})$的基数,$(\frac{\triangle}{p})$表Kronecker符号。

Ⅴ. 下面介绍在解丢番图方程时经常用到的结果。

设 A, B是$Q(\theta)$上的理想数, 如果存在α, $\beta\in Z[\theta]$使

得

$$[\alpha]A=[\beta]B,$$

则称A，B同属一个理想数类，记为$A\sim B$。由此关系可将$Q(\theta)$上的全体理想数分类，其类数h是一个有限正整数，称为$Q(\theta)$的理想类数(简称$Q(\theta)$的类数)。我们有：任给$Q(\theta)$中的理想数A，总有$\alpha\in Z[\theta]$使得

$$A^h=[\alpha]。$$

由此立即推出：如果$(l,h)=1$，A^l是一个主理想数，则A是一个主理想数。

这个结果是我们解丢番图方程

$$xy=cz^l,\quad (x,y)=1 \tag{3}$$

的主要依据，这里x，y，$z\in Z[\theta]$是变元，$c\in Z[\theta]$是给定的。

例1 设$Q(\theta)$中的理想类数为h，$(l,\ h)=1$，则丢番图方程(3)在$Z[\theta]$上的全部解可表为

$$x=\xi_1c_1\alpha^l,\quad y=\xi_2c_2\beta^l,\quad z=\xi_3\alpha\beta, \tag{4}$$

这里$\xi_1\xi_2=\xi_3{}^l$，$c_1c_2=c$且，ξ_1,ξ_2,ξ_3是$Q(\theta)$中的单位数，c_1，c_2，α，$\beta\in Z[\theta]$，$(c_1,c_2)=(\alpha,\ \beta)=1$。

证 为了使(3)式得到展开，我们把(3)化为理想数方程

$$[x][y]=[c][z]^l。$$

由理想数的唯一分解定理(Ⅲ)知，上式给出

$$[x]=[c_1]A^l,\quad [y]=[c_2]B^l,\quad [z]=AB, \tag{5}$$

这里$[c]=[c_1][c_2]$，$(c_1,c_2)=1$。由$(h,\ l)=1$知，A，B均是$Q(\theta)$上的主理想数（看Ⅴ）。设$A=[\alpha]$，$B=[\beta]$，α，$\beta\in Z[\theta]$，则(5)式给出

$$[x]=[c_1\alpha^l],\quad [y]=[c_2\beta^l],\quad [Z]=[\alpha\beta],$$

由此即得方程(3)的解(4)，证毕。

例1 的结果是我们利用代数数论解丢番图方程的一般思路。在一些特殊的问题中，常常只用到二次域$Q(\sqrt{D})$的情形。设$h(D)$表示$Q(\sqrt{D})$中的理想类数，则在$D<0$时$h(D)=1 \Longleftrightarrow D=-1$，$-2$，$-3$，$-7$，$-11$，$-19$，$-43$，$-67$，$-163$。下面我们举几个在二次域$Q(\sqrt{D})(h(D)=1)$中考虑的丢番图方程的例子，以说明代数数论方法的应用。

例2 设$n>1$，则丢番图方程

$$1+x^2=y^n \tag{6}$$

没有正整数解。

证 显然n不能为偶数，所以不妨设n为奇素数，由(6)显然$y\equiv 1\pmod 2$，$x\equiv 0 \pmod 2$。现把方程(6)化为$Q(\sqrt{-1})$中的方程

$$(1+x\sqrt{-1})(1-x\sqrt{-1})=y^n。$$

设 $d=(1+x\sqrt{-1},\ 1-x\sqrt{-1})$，则 $d\mid 2$，$d\mid 1+x\sqrt{-1}$，推出$d\mid 1$，故$d=1$。由于$h(-1)=1$，所以由例1的结果知，上式给出

$$1+x\sqrt{-1}=\xi_1\ (u+v\sqrt{-1})^n,\quad y=u^2+v^2, \tag{7}$$

这里ξ_1为$Q(\sqrt{-1})$中的单位数。由Ⅱ知，$Q(\sqrt{-1})$的单位数有± 1，$\pm i$。显然，当$\xi_1=\pm 1$时可归并到(7)式右端的括号内；又由于当$n\equiv 1 \pmod 4$时$i=i^n$，当$n\equiv 3\pmod 4$时$i=(-i)^n$，故$\xi_1=\pm i$仍可归并到(7)式右端的括号内。这样，不失一般可设$\xi_1=1$，由(7)式利用二项式定理展开，得出

$$\begin{aligned}1&=\frac{(u+v\sqrt{-1})^n+(u-v\sqrt{-1})^n}{2}\\&=\sum_{0\leqslant j\leqslant\frac{n-1}{2}}\binom{n}{2j}u^{n-2j}(v\sqrt{-1})^{2j},\end{aligned} \tag{8}$$

由此知$u|1$，所以$u=\pm 1$。

如果$u=-1$，则(8)给出

$$-2=\sum_{1\leqslant j\leqslant\frac{n-1}{2}}\binom{n}{2j}(v\sqrt{-1})^{2j},$$

由于n是奇素数，$n\left|\binom{n}{2j}\right.$ $\left(1\leqslant j\leqslant\frac{n-1}{2}\right)$，故上式推出$n|2$，这不可能。

如果$u=1$，则(8)给出

$$0=\sum_{1\leqslant j\leqslant\frac{n-1}{2}}\binom{n}{2j}(v\sqrt{-1})^{2j} \tag{9}$$

由 $y=u^2+v^2$，$2\nmid y$ 知$2|v$。故用比较素数幂法(见第二章§4)知，(9)给出$v=0$，从而$y=1$，$x=0$，非(6)的正整数解。证毕。

例3 证明丢番图方程

$$y^3=4^z+x^2,(x,y)=1 \tag{10}$$

仅有正整数解$(x,y,z)=(11,\ 5,\ 1)$。

证 如果(10)有正整数解，则显然，$2\nmid x$，$y\equiv 1(\bmod 4)$。由(10)得

$$(2^z+x\sqrt{-1})(2^z-x\sqrt{-1})=y^3,$$

因为$2\nmid x$，所以上式给出

$$2^z+x\sqrt{-1}=(u+v\sqrt{-1})^3,\quad y=u^2+v^2,$$

由此即知

$$2^z=u(u^2-3v^2),$$

由$y\equiv 1(\bmod 4)$知u，v一奇一偶，因此上式给出

$$u=\pm 2^z,\quad u^2-3v^2=\pm 1,$$

此即

$$2^{2z}-3v^2=1,$$

对此取模8 知，$z=1$，$v^2=1$，给出$y=5$，$x=11$，即得方程(10)仅有正整数解

$$(x,\ y,\ z)=(11,\ 5,1)$$ 。证毕。

例4 丢番图方程

$$x^2+7=2^y \tag{11}$$

仅有正整数解

$(x,y)=(1,\ 3)$，$(3,\ 4)$，$(5,\ 5)$，$(11,\ 7)$，$(181,\ 15)$。

证 显然(11)给出$y\geqslant 3$。我们在二次域$Q(\sqrt{-7})$中来考虑方程(11)。由于$Q(\sqrt{-7})$有一组整底$1,\dfrac{1+\sqrt{-7}}{2}$（见Ⅱ），故$Q(\sqrt{-7})$中的整数皆具有$\dfrac{u+v\sqrt{-7}}{2}$的形状，这里$u\equiv v\pmod 2$。于是把(11)改写为$Q(\sqrt{-7})$中整数所满足的方程

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)=2^n,\quad y=n+2。\tag{12}$$

我们来证明$\left(\dfrac{x+\sqrt{-7}}{2},\ \dfrac{x-\sqrt{-7}}{2}\right)=1$。设$d=\left(\dfrac{x+\sqrt{-7}}{2},\ \dfrac{x-\sqrt{-7}}{2}\right)$，则$d\mid\dfrac{x+\sqrt{-7}}{2}-\dfrac{x-\sqrt{-7}}{2}=\sqrt{-7}$。由于$\sqrt{-7}$是$Q(\sqrt{-7})$中的素数，故$d=1$或$\sqrt{-7}$。如果$d=\sqrt{-7}$，则由$d\mid\dfrac{x+\sqrt{-7}}{2}+\dfrac{x-\sqrt{-7}}{2}=x$知$7=N(\sqrt{-7})\mid x^2$，得出$7\mid x$，这而由(11)知，显然不可能。于是$d=1$。这样，由$h(-7)=1$知，(12)

给出

$$\pm\frac{x+\sqrt{-7}}{2}=\omega^n,\ 或\pm\frac{x-\sqrt{-7}}{2}=\omega^n, \tag{13}$$

其中 $\omega=\frac{1+\sqrt{-7}}{2}$。令 $\overline{\omega}=\frac{1-\sqrt{-7}}{2}$，$b_n=\frac{\omega^n-\overline{\omega}^n}{\omega-\overline{\omega}}$，

则由于(13)给出

$$\pm\left(\frac{x-1}{2}+\omega\right)=\omega^n,\ 或\pm\left(\frac{x+1}{2}-\omega\right)=\omega^n$$

知 $b_n=\pm1$。而我们在第二章§7的例4中证明了

$b_n=\pm1\Longleftrightarrow n=1,2,3,5$ 和13,

故方程(11)仅有正整数解 $(x,y)=(1,3),(3,4),(5,5),(11,7),(181,15)$。证毕。

例5 设 $D(\neq1)$ 无平方因子，p 为奇素数且 $p\nmid D$。如果丢番图方程

$$x^2-Dy^2=p^z,\ (x,y)=1 \tag{14}$$

有正整数解，可设 (x_0,y_0,z_0) 是(14)的正整数解中使 z 为最小的一组解（称为最小解），则(14)的全部解可表为

$$x+y\sqrt{D}=\varepsilon(x_0+y_0\sqrt{D})^t 或 \varepsilon(x_0-y_0\sqrt{D})^t,$$

$$z=z_0t,\ 0<t\in Z,\ \varepsilon 为 Q(\sqrt{D}) 的任意单位数。$$

证 在二次域 $Q(\sqrt{D})$ 中分解(14)式得

$$(x+y\sqrt{D})(x-y\sqrt{D})=p^z \tag{15}$$

因为 $(x,y)=1$，p 为奇素数且 $p\nmid D$，故易知 $(x+y\sqrt{D},x-y\sqrt{D})=1$。又因为假设(14)有解，故有 $\left(\frac{D}{p}\right)=1$。

因此，由Ⅳ知$[p]$在$Q(\sqrt{D})$中可分解为：$[p]=P\overline{P}$，$P\neq\overline{P}$且$N(P)=N(\overline{P})=p$。现把(15)改写成理想数方程，得出

$$[x+y\sqrt{D}][x-y\sqrt{D}]=[p]^z=P^z\overline{P}^z。 \tag{16}$$

故由理想数的唯一分解定理知，(16)式给出

$$[x+y\sqrt{D}]=P^z \quad 或 \quad [x+y\sqrt{D}]=\overline{P}^z, \tag{17}$$

这就有P^z或$\overline{P}^z$是一个主理想数。由假设知$P^{z_0}=[x_0+y_0\sqrt{D}]$或$[x_0-y_0\sqrt{D}]$，写$z=tz_0+r$，$0\leqslant r<z_0$，则$P^r$是一个主理想数。故由$z_0$的最小性知$r=0$，于是$z=tz_0$，且(17)化为

$$[x+y\sqrt{D}]=[x_0+y_0\sqrt{D}]^t或[x_0-y_0\sqrt{D}]^t,$$

由此即得(14)的解。证毕。

显然，在例5中，如果$D<0$，$D\neq-1,-3$，则$Q(\sqrt{D})$中的单位数为±1，故$\varepsilon=\pm1$；如果$D>0$，$D\neq1$，则$Q(\sqrt{D})$的单位数为$\pm\eta^n$，$n\in Z$，η为$Q(\sqrt{D})$的基本单位数，故$\varepsilon=\pm\eta^n$。

例5 的结果（当$D<0$）在许多丢番图方程的研究中都有应用，例如，曹珍富给出它对 Hall 方程$p^m-q^n=2$、Hugh Edgar 方程$\dfrac{p^x-1}{p-1}=q^y$和$p^m-q^n=2^h$（这里p,q均表素数）的应用（参见第九章§1和第八章§3），得出了一系列的结果（见[1]、[2]和[3]）。

利用代数数论方法，还可以处理一般的丢番图方程

$$x^2-Dy^4=k,\quad D>0非平方数 \tag{18}$$

和

$$x^4-Dy^2=k,\quad D>0非平方数 \tag{19}$$

（参阅第七章§4）。例如，对方程（18），可设$D=e^2d$，$d>1$无平方因子。在二次域$Q(\sqrt{d})$中，令

$$(a,\ b)=\begin{cases}(x,ey^2), & \text{当} d\equiv 2,3(\bmod\ 4);\\ (x-ey^2,2ey^2), & \text{当} d\equiv 1(\bmod\ 4)。\end{cases}$$

则

$$N(a+b\omega)=k, \tag{20}$$

这里

$$\omega=\begin{cases}\sqrt{d}, & \text{当} d\equiv 2,3(\bmod\ 4);\\ \dfrac{1+\sqrt{d}}{2}, & \text{当} d\equiv 1(\bmod\ 4)。\end{cases}$$

于是，在$Z[\omega]$中，我们可以找到一个有限子集K和一个单位数ε，使得

$$N(\eta)=k,\ \eta\in K \text{ 和 } N(\varepsilon)=1。$$

所以（20）推出

$$a+b\omega=\pm\eta\varepsilon^n,\ \text{对某些}\eta\in K,\ n\in Z。\tag{21}$$

设$n=2m+j$，$j\in\{0,1\}$，令

$$\eta\varepsilon^j=s+t\omega,\quad \varepsilon^m=u+v\omega,\quad s,t,u,v\in Z,$$

则由（21）给出

$$a+b\omega=\pm\eta\varepsilon^j\cdot\varepsilon^{2m}=\pm(s+t\omega)(u+v\omega)^2.$$

由此推出：

1）当$d\equiv 2,3(\bmod\ 4)$时，我们有

$$\pm ey^2=tu^2+2suv+tdv^2;$$

2）当$d\equiv 1(\bmod\ 4)$时，我们有

$$\pm 2ey^2=tu^2+2(s+t)uv+\left(s+\frac{d+3}{4}\cdot t\right)v^2。$$

这就使方程(18)得到了展开。

习　　题

1．证明丢番图方程

$$x^2+7^y=2^z$$

仅有正整数解$(x,y,z)=(1,1,3),(3,1,4)$，$(5,1,5)$，$(11,1,7)$，$(181,1,15)$和$(13,3,9)$。

2．设$D>2$，$Q(\sqrt{-D})$的类数h满足$(n,h)=1$，则丢番图方程

$$x^n-Dy^2=1,\quad n>2$$

如有正整数解，必有$2\mid x$。

3．证明丢番图方程

$$x^2+2=y^n,\quad n>2$$

仅有正整数解$x=5$，$y=3$，$n=3$。

4．证明$x^2+11=4y^5$仅有正整数解$x=31$，$y=3$。

5．设$D\neq 1$无平方因子，$Q(\sqrt{D})$的类数不被3整除，且$Q(\sqrt{D})$的素数没有一个整除$2m$，则丢番图方程$y^2-Dm^2=x^3$给出$\pm y+m\sqrt{D}=\mu\alpha^3$，这里$\alpha$是$Q(\sqrt{D})$中的整数且$\mu$是$Q(\sqrt{D})$的基本单位或1。

§2　代数数论方法(Ⅱ)

在§1中我们讨论了把丢番图方程放到代数整环中研究的一些方法，这个方法的实质是利用代数数论的一些知识把丢番图方程化成若干容易处理的方程。这一节，我们将利用域$Q(\sqrt{-3})$中代数整数的性质，引进三次剩余特征的概念，利用三次剩余的一些结果来解某些含有x^3+y^3形的丢番图方程。相应地，引进l次剩余特征可以解某些高次的丢番图方程。

Ⅰ. 设$\omega=\frac{-1+\sqrt{-3}}{2}$, $\omega^2+\omega+1=0$, 由二次域$Q(\sqrt{-3})$的知识知, $Q(\sqrt{-3})$中的全体整数组成的整环$Z[\sqrt{-3}\ ]=Z[\omega]$, 这里$Z[\omega]$称为Eisenstein 环, 由下式定义

$$Z[\omega]=\{a+b\omega \mid a,b\in Z\}。$$

在域$Q(\sqrt{-3})$中, 整数为$a+b\omega$, a, $b\in Z$, 单位数为$\pm\omega^n$ $(n=0,\ 1,2)$, 素数为:

1) 有理素数$q\equiv-1 \pmod 3$是素数;

2) 如果有理素数$p\equiv1 \pmod 3$, 则$p=N(\pi)=\pi\pi'$ $=a^2-ab+b^2$的因子$\pi=a+b\omega$, $\pi'=a+b\omega^2$均为素数;

3) $\lambda=1-\omega$为素数, 这里$\lambda^2=-3\omega$。

设$\pi\in Z[\omega]$是素数, $N(\pi)\neq3$, $\pi\nmid\alpha\in Z[\omega]$, 则$N(\pi)\equiv 1 \pmod 3$, $\alpha^{N(\pi)-1}\equiv1 \pmod \pi$, 由此推出存在唯一的$t=0$, 1或2, 使得

$$\alpha^{\frac{N(\pi)-1}{3}}\equiv\omega^t \pmod \pi。\qquad (1)$$

于是, 定义α对模π的三次剩余特征为

$$\left(\frac{\alpha}{\pi}\right)_3=\omega^t,$$

其中t满足(1)式。现在我们引进本原数的概念。如果$x\equiv-1 \pmod 3$, $y\equiv0 \pmod 3$, 则称$x+y\omega$为本原数。很显然, 任给整数$a+b\omega\in Z[\omega]$, 均可写成$\pm\omega^n\cdot\lambda^m$与一个本原数的乘积。因此, 任意$\alpha\in Z[\omega]$, α均可分解为

$$\alpha=(-1)^u\omega^v\lambda^w\pi_1^{a_1}\cdots\pi_s^{a_s},$$

其中u, $v,w,a_j(j=1,\ \cdots,s)$均为非负整数, $\lambda=1-\omega,\pi_j$

$(j=1,\cdots,s)$是本原素数。由此可见，计算$\left(\frac{\alpha}{\pi}\right)_3$

归结为计算$\left(\frac{-1}{\pi}\right)_3$，$\left(\frac{\omega}{\pi}\right)_3$，$\left(\frac{1-\omega}{\pi}\right)_3$，和$\left(\frac{\pi_j}{\pi}\right)_3$。

在 $\pi \nmid \alpha$ 时，我们有

$$\left(\frac{-1}{\pi}\right)_3=1,\left(\frac{\pi_j}{\pi}\right)_3=\left(\frac{\pi}{\pi_j}\right)_3;$$

设$\pi=a+b\omega$，$a=3m-1$，$b=3n$，则有

$$\left(\frac{\omega}{\pi}\right)_3=\omega^{m+n}，\left(\frac{1-\omega}{\pi}\right)_3=\omega^{2m}。$$

因为在$\pi \nmid \alpha\beta$时，易知$\left(\frac{\alpha\beta}{\pi}\right)_3=\left(\frac{\alpha}{\pi}\right)_3\left(\frac{\beta}{\pi}\right)_3$，故由

$(1-\omega)^2=-3\omega$有

$$\omega^{4m}=\left(\frac{1-\omega}{\pi}\right)_3^2=\left(\frac{-3\omega}{\pi}\right)_3=\left(\frac{3}{\pi}\right)_3\omega^{m+n},$$

注意到$\omega^3=1$，我们得到

$$\left(\frac{3}{\pi}\right)_3=\omega^{2n}。$$

由于

$$\left(\frac{\pi}{2}\right)_3=\left(\frac{2}{\pi}\right)_3,$$

故容易推出$\left(\frac{2}{\pi}\right)_3=1 \Leftrightarrow \pi\equiv a \pmod 6$。下面我们利用三次剩余特征来解若干丢番图方程。

例1 丢番图方程

$$x^3+y^3+2z^3=1 \tag{2}$$

如有整数解，则$6|x$或$6|y$。

证 对方程(2)取模9知$3|xy$，不妨设$3|y$，此时$x\equiv\pm1 \pmod 3$。在$Z[\omega]$中，方程(2)可改写为

$$(x+y)(x+\omega y)(x+\omega^2 y)+2z^3=1. \tag{3}$$

由于$x+y\omega$可分解为

$$x+y\omega=\pm\pi_1\cdots\pi_t,$$

其中$\pi_j(j=1,\cdots,t)$均为本原素数，且$N(\pi_j)\neq3(j=1,\cdots,t)$，故(3)式给出

$$(2z)^3\equiv4 \pmod{\pi_j} \quad (j=1,\cdots,t),$$

所以

$$1=\left(\frac{4}{\pi_j}\right)_3=\left(\frac{2}{\pi_j}\right)_3^2 \quad (j=1,\cdots,t),$$

故得出$\pi_j\equiv a_j \pmod 6$，$a_j\in Z(j=1,\cdots,t)$，所以

$$x+y\omega\equiv\pm a_1\cdots a_t \pmod 6,$$

由此推出$6|y$。同理，若$3|x$，则推出$6|x$。证毕。

例2 丢番图方程

$$x^3+y^3+z^3=3 \tag{4}$$

如有正整数解，则$x\equiv y\equiv z \pmod 9$。

证 对方程(4)取模9知$x\equiv y\equiv z\equiv1 \pmod 3$。改写方程(4)为

$$(x+y)(x+\omega y)(x+\omega^2 y)+z^3=3。 \tag{5}$$

由于$\omega(x+\omega y)\equiv2 \pmod 3$，故$x+\omega y$可分解为

$$x+\omega y=\pm\omega^2\pi_1\cdots\pi_t,$$

其中$\pi_j(j=1,\cdots,t)$是本原素数。所以(5)给出

$$z^3\equiv3 \pmod{\pi_j} \quad (j=1,\cdots,t)。$$

由于(4)给出$3\nmid x^3+y^3$，故$\pi_j\nmid3(j=1,\cdots,t)$，上式给出

$$1=\left(\frac{3}{\pi_j}\right)_3=\omega^{2n_j}\quad (j=1,\ \cdots,t),$$

这里设$\pi_j=3m_j-1+3n_j\omega$ $(j=1,\cdots,t)$。由此即得

$n_j\equiv 0\pmod 3$ $(j=1,\cdots,t)$，$\pi_j\equiv 3m_j-1\pmod 9$ $(j=1,\cdots,t)$。于是

$$\omega(x+\omega y)\equiv \pm(3m_1-1)\cdots(3m_t-1)\pmod 9,$$

即

$$-y+(x-y)\omega\equiv \pm(3m_1-1),\cdots(3m_t-1)\pmod 9$$

所以 $x\equiv y\pmod 9$。同理可证$y\equiv z\pmod 9$。证毕。

方程(4)现在已知有四个解$(x,y,z)=(1,1,1),(4,4,-5)$，$(4,-5,4)$和$(-5,4,4)$，它们显然都满足$x\equiv y\equiv z\pmod 9$。但方程(4)是否还有别的解？这是一个困难的未解决问题。

例3 设$p\equiv 2,5\pmod 9$是素数，则丢番图方程

$$x^3+y^3=pz^3,\quad z\neq 0 \tag{6}$$

在$Z[\omega]$中除$p=2$，$x^3=y^3=z^3$外，无其他的解。

证 若(6)有解，不妨设$(x,y)=1$，且x,y,z是(6)的所有解中使$N(xyz)$为最小的一组解。在$Z[\omega]$中，方程(6)可分解为

$$(x+y)(x+y\omega)(x+y\omega^2)=pz^3。 \tag{7}$$

令$\alpha=x+y$，$\beta=x\omega+y\omega^2$，$\gamma=x\omega^2+\omega y$，则

$$\delta=(\alpha,\beta,\gamma)=1,1-\omega或1-\omega^2,$$

所以由(7)得出

$$\frac{\alpha}{\delta}\cdot\frac{\beta}{\delta}\cdot\frac{\gamma}{\delta}=p\cdot\left(\frac{z}{\delta}\right)^3。 \tag{8}$$

由于易知$\frac{\alpha}{\delta}$、$\frac{\beta}{\delta}$、$\frac{\gamma}{\delta}$两两互素，故不失一般性设$p\mid\frac{\gamma}{\delta}$，(8)给出

$$\frac{\alpha}{\delta}=\varepsilon_1 x_1^3,\quad \frac{\beta}{\delta}=\varepsilon_2 y_1^3,\quad \frac{\gamma}{\delta}=p\varepsilon_3 z_1^3,$$

这里$\varepsilon_1,\varepsilon_2,\varepsilon_3$是$Z[\omega]$中的单位数，$\varepsilon_1\varepsilon_2\varepsilon_3=1$，且$x_1y_1z_1=\frac{z}{\delta}\neq 0$。由于 $\alpha+\beta+\gamma=(x+y)+(x\omega+y\omega^2)+(x\omega^2+\omega y)=0$，故得

$$\varepsilon_1 x_1^3+\varepsilon_2 y_1^3+p\varepsilon_3 z_1^3=0,\quad \varepsilon_1\varepsilon_2\varepsilon_3=1, \tag{9}$$

由于$\left(\frac{\varepsilon_1}{p}\right)_3=\left(\frac{-\varepsilon_2}{p}\right)_3=\left(\frac{\varepsilon_2}{p}\right)_3$，故$\varepsilon_1=\pm\varepsilon_2$，所以(9)式给出

$$x_1^3\pm y_1^3=p\eta z_1^3,\quad \eta=\mp 1,$$

即得出x_1，$\pm y_1$，$\mp z_1$为方程(6)的解。故

$$N(xyz)\leqslant N(x_1y_1z_1)=N\left(\frac{z}{\delta}\right)。$$

由此得出$N(\delta xy)\leqslant 1$，所以$N(\delta xy)=1$，δ，x,y均是单位数，即$x^3=\pm 1$，$y^3=\pm 1$。由x，y的假设推知，方程(6)在$p>2$时$z=0$，这不可能；在$p=2$时仅有$x^3=y^3=z^3$。证毕。

由例3立即推出：设$p\equiv 2,5 \pmod 9$是素数，则丢番图方程

$$x^3+y^3=pz^3,\qquad z\neq 0$$

除$p=2$，$x=y=z$外，无其他的整数解。

利用$Q(\sqrt{-3})$中整数的一些性质还可以解一些形如

$$ax^3+by^3+cz^3-dxyz=0 \tag{10}$$

的丢番图方程。令$X=ax^3$，$Y=by^3$，$Z=cz^3$，$W=xyz$，则(10)可化为求如下两个方程的公解：

$$X+Y+Z=dW, \tag{11}$$

$$XYZ = eW^3。\qquad (12)$$

求方程(10)的有理数解与求其整数解是等价的，但求(11)和(12)的有理数公解，却是特别的困难，即使对于 $W=1$ 也是如此。

在 $Q(\sqrt{-1})$ 中，可以引入四次剩余特征的概念，利用四次剩余特征也可解一些丢番图方程。由于这个概念在解丢番图方程时，常常是只用到 $\left(\frac{2}{p}\right)_4$ ($p\equiv 1 \pmod 4$ 为有理素数) 的结果，或等价于直接取正整数模，而这些在第二章的§1中已经介绍过了，故这里从略。

Ⅱ. 设 m 是一个正整数，D_m 表示 m 次分圆域 $Q(\xi_m)$ ($\xi_m = e^{2\pi i/m}$) 中的整数环。P 是一个不包含 m 的素理想，则对 $\alpha \in D_m$，定义 m 次剩余符号 $\left(\frac{\alpha}{P}\right)_m$ 为：

a) $\left(\frac{\alpha}{P}\right)_m = 0$，当 $\alpha \in P$；

b) 如果 $\alpha \notin P$，则 $\left(\frac{\alpha}{P}\right)_m$ 是一个 m 次的单位根，

满足 $\left(\frac{\alpha}{P}\right)_m \equiv \alpha^{(N(P)-1)/m} \pmod P$。这里 $N(P) = |D_m/P|$，$|A|$ 表集 A 的元素个数。

根据这个定义，我们有如下结果：

1) 设 P 是不包含 m 的素理想，则 $\left(\frac{\xi_m}{P}\right)_m = \xi_m^{(N(P)-1)/m}$。

为了介绍Eisenstein互反律，下面设 l 是一个奇素数。在 D_l 中，我们有 $[l] = [1-\xi_l]^{l-1}$ 并且 $[1-\xi_l]$ 是一个次数

为1的素理想。与三次剩余一样，引进本原数的概念是重要的。一个非零元$\alpha\in D_l$被称为本原数，如果α与l互素，且$\alpha\equiv a(\mathrm{mod}(1-\xi_l)^2)$，这里$a\in Z$。

2）设l是一个奇素数，$a\in Z$与l互素，且$\alpha\in D_l$是一个本原数。如果α与a互素，则有

$$\left(\frac{\alpha}{a}\right)_l=\left(\frac{a}{\alpha}\right)_l。$$

现在我们利用Eisenstein互反律2）来解Fermat方程

$$x^l+y^l+z^l=0,\ l\text{是奇素数},\ (x,\ y,\ z)=1。\quad (13)$$

我们知道，1909年A. Wieferich[15]曾得到关于方程(13)的一个重要结果：如果方程(13)有非零整数解，$l\nmid xyz$，则$2^{l-1}\equiv1(\mathrm{mod}\ l^2)$。1912年，Furtwängler改进了Wieferich的结果，证明了

例 4 如果方程(13)有非零整数解，$l\nmid yz$，则对y的任一个素因子p有$p^{l-1}\equiv1(\mathrm{mod}\ l^2)$

证 由方程(13)得

$$(x+y)(x+\xi_l y)\cdots(x+\xi_l^{l-1}y)=(-z)^l。\quad (14)$$

首先可证$x+\xi_l^i y$与$x+\xi_l^j y$（这里$i\neq j$，$0\leqslant i,j<l$）在D_l中是互素的，因此(14)的左端给出的每一个理想$[x+\xi_l^i y]$都是一个l次幂。

考虑$\alpha=(x+y)^{l-2}(x+\xi_l y)$，显然有$[\alpha]$是一个$l$次幂。由于$x+\xi_l y=x+y-y\lambda$，故$\alpha\equiv(x+y)^{l-1}-\lambda u$，这里$u=(x+y)^{l-2}y$。现在$x^l+y^l+z^l\equiv x+y+z(\mathrm{mod}\ l)$，如$l\mid x+y$，则$l\mid z$，而这是不可能的；因此$l\nmid x+y$，给出$(x+y)^{l-1}\equiv1(\mathrm{mod}\ l)$，故$\alpha\equiv1-u\lambda(\mathrm{mod}\lambda^2)$。对于$\xi_l^{-u}\alpha$，我们有$\xi_l^{-u}\alpha=(1-\lambda)^{-u}\alpha\equiv(1+u\lambda)(1-u\lambda)\equiv1(\mathrm{mod}\ \lambda^2)$。因而$\xi_l^{-u}\alpha$是本原数，故由Eisenstein互反律得

$$\left(\frac{p}{\xi_l^{-u}\alpha}\right)_l=\left(\frac{\xi_l^{-u}\alpha}{p}\right)_l=\left(\frac{\xi_l}{p}\right)_l^{-u}\left(\frac{\alpha}{p}\right)_l 。\qquad (15)$$

因为理想$[\xi_l^{-u}\alpha]=[\alpha]$是一个$l$次幂，因此(15)式$=1$，又由$p|y$，$\alpha\equiv(x+y)^{l-1}(\bmod\ p)$知

$$\left(\frac{\alpha}{p}\right)_l=\left(\frac{(x+y)^{l-1}}{p}\right)_l=\left(\frac{p}{(x+y)^{l-1}}\right)_l=1,$$

因此(15)式给出

$$\left(\frac{\xi_l}{p}\right)_l^u=1。$$

设$pD_l=P_1P_2\cdots P_g$是p在D_l中的素数分解。已知$N(P_i)=p^f$且$gf=l-1$（因为$p\neq l$，$e=1$），故由1)知

$$\left(\frac{\xi_l}{p}\right)_l=\prod_{i=1}^{g}\left(\frac{\xi_l}{P_i}\right)_l=\prod_{i=1}^{g}\xi_l^{(p^f-1)/l}=\xi_l^{g[(p^f-1)/l]}。$$

由$\left(\frac{\xi_l}{p}\right)_l^u=1$知，上式给出

$$1=\xi_l^{ug[(p^f-1)/l]},$$

此即 $ug\frac{p^f-1}{l}\equiv0(\bmod\ l)$。因$g|l-1$，故$l\nmid g$。又因$u=(x+y)^{l-2}y$，$l\nmid u$，故有 $\frac{p^f-1}{l}\equiv0\ (\bmod\ l)$ 或 $p^f\equiv1\ (\bmod\ l^2)$。由于$f|l-1$，故$p^{l-1}\equiv1(\bmod\ l^2)$。证毕。

习　　题

1. 若丢番图方程$x^3+y^3+z^3=2$有解，则必有6整除x，y，z，中的一个。

2. 如果丢番图方程

$$x^3+y^3+z^3=9$$

有正整数解，则必有9整除x,y,z中的一个。

3. 在$Z[\omega]$中，证明丢番图方程

$$x^3+y^3=2pz^3,\quad p\equiv5(\mathrm{mod}\ 18)\text{是素数},\quad z\neq0$$

无解。

4. 在$Z[\omega]$中，证明丢番图方程

$$x^3+y^3=z^3,\quad xyz\neq0$$

无解。

5. 证明丢番图方程

$$x^3+y^3+z^3=6,\quad 2|z$$

的整数解满足$x\equiv y(\mathrm{mod}\ 18)$。

§3 p—adic 方法

有一大类丢番图方程都可以化为

$$N(x_1\omega_1+\cdots+x_n\omega_n)=a \tag{1}$$

的形式，其中$\omega_1,\cdots,\omega_n$是n次代数数域$Q(\theta)$的整底，$N(\omega)$为ω的范数，a为给定的有理整数。利用代数数论的知识（参阅§1），方程(1)可以化为

$$x_1\omega_1^{(j)}+\cdots+x_n\omega_n^{(j)}=c^{(j)}\varepsilon^{(j)}(j=1,\cdots,n), \tag{2}$$

这里$\omega^{(j)}(j=2,\cdots,n)$表示$\omega(=\omega^{(1)})$的共轭，$c^{(j)}$和$\varepsilon^{(j)}$分别满足$N(c^{(j)})=a$和$N(\varepsilon^{(j)})=1$且$c^{(j)}$只取有限个$Q(\theta)$中的整数。由(2)比较$\omega_1^{(j)},\cdots,\omega_n^{(j)}$的系数可以得出若干等式，有一部分等式是

$$g_l(x_1,\cdots,x_n)=0(l=1,\cdots,n-m),$$

其中m是一给定正整数，g_l是关于$x_1,\cdots,x_n$的有理系数多项式。然后利用p—adic数的性质可以给出方程的全部解。

为了说明这个方法，我们引进p-adic数域Q_p和p-adic整数环Z_p的概念，这里的p表素数。

我们首先引进p-adic赋值的概念。在有理数域Q上，$x \in Q$，所谓p-adic赋值$|x|_p$定义为：

$$|x|_p = \begin{cases} 0, & \text{当} x = 0; \\ p^{-\alpha}, & \text{当} x = p^{\alpha}\dfrac{x_1}{x_2}, (x_1, x_2) = 1 \text{且} p \nmid x_1 x_2。\end{cases}$$

显然，p-adic赋值有如下的性质：

1) $|x|_p \geqslant 0$，且$|x|_p = 0 \Longleftrightarrow x = 0$；

2) $|x_1 x_2|_p = |x_1|_p |x_2|_p$；

3) $|x_1 \pm x_2|_p \leqslant |x_1|_p + |x_2|_p$。

第3)条性质还可以加强为

$$|x_1 \pm x_2|_p \leqslant \max(|x_1|_p, |x_2|_p)。$$

一个Q上的p-adic收敛序列$\{x_n\}$：

$$x_1, \ x_2, \ \cdots, \ x_n, \ \cdots,$$

这里$x_n \in Q$，定义为：对任给的$\varepsilon > 0$，存在$L(\varepsilon)$使得当m，$n \geqslant L(\varepsilon)$时，有

$$|x_m - x_n|_p < \varepsilon$$

成立。如果上式换为$|x_n - a|_p < \varepsilon$，则称$p$-adic收敛序列$\{x_n\}$收敛于$a(a \in Q)$。如果两个$p$-adic收敛序列$\{x_n\}$和$\{y_n\}$之差$\{x_n - y_n\}$收敛于0，则称$\{x_n\}$和$\{y_n\}$属于一类。由所有$p$-adic收敛序列的所有不同类构成的集合称为$p$-adic数系，称$p$-adic数系中的每一个$p$-adic序列所对应的$p$-adic幂级数为一个$p$-adic数。所有$p$-adic数构成一域，称为$p$-adic域。显然，对任意$x \in Q_p$，则$x$有以下的形式：

$x = p^{-m}(a_0 + a_1 p + a_2 p^2 + \cdots)$，$0 \leqslant a_i < p (i = 0, 1, \cdots)$，$m \geqslant 0$，

其中幂级数可以是有限的或无限的。如果$|x|_p \leqslant 1$，则x称为

Q_p中的整数(p-adic整数)，全体p-adic整数构成一环，称为p-adic整环Z_p。Z_p中可逆元素称为p-adic单位。

幂级数的收敛性判断是十分简单的。因为级数$\sum a_n$收敛$\Leftrightarrow |a_n|_p \to 0$。于是可知，如果$|a_n|_p \to 0$，则$f(x)=\sum_{n=0}^{\infty} a_n x^n$在$|x|_p \leqslant 1$时收敛。指数和对数函数的展开式为

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots \left(|x|_p < \frac{1}{p-1} \right),$$

$$\log(1+x) = x - \frac{x^2}{2} + \cdots + \frac{(-1)^{n-1} x^n}{n} + \cdots (|x|_p < 1)。$$

以上讨论的情况可以把Q换为一般的代数数域$Q(\theta)$。如果ε是$Q(\theta)$的单位，则存在有理整数a满足

$$\varepsilon^a \equiv \begin{cases} 1 (\mathrm{mod}\ \ p)，当p为奇素数； \\ 1 (\mathrm{mod}\ \ 4)，当p=2。 \end{cases}$$

令$\varepsilon^a = 1 + p\xi$，则由于$|p\xi|_p < 1$，故

$$\log \varepsilon^a = p\xi - \frac{(p\xi)^2}{2} + \cdots + \frac{(-1)^{n-1}(p\xi)^n}{n} + \cdots,$$

因此对任意p-adic整数x，我们可将

$$\varepsilon^{xa} = e^{x \log \varepsilon^a}$$

展开为系数属于$Q(\theta)$的幂级数。由于对任意u，可写$u = av + b$，$0 \leqslant b < a$，故我们可以将ε^u展开为系数属于$Q(\theta)$的幂级数。

下面我们通过若干实例来说明p-adic方法在解形如(1)(或可化为(1))的丢番图方程中的应用。

例1 设$d > 1$是一个给定的整数，则丢番图方程

$$x^3 + dy^3 = 1, \quad xy \neq 0 \tag{3}$$

最多有一组整数解。

证 假设(3)有两组不同的整数解(x_1, y_1)，(x_2, y_2)，$x_iy_i \neq 0 (i=1, 2)$。令$\theta = \sqrt[3]{d}$，则$\varepsilon_1 = x_1 + y_1\theta$和$\varepsilon_2 = x_2 + y_2\theta$都是域$Q(\theta)$中的单位数，且$N(\varepsilon_1) = N(\varepsilon_2) = 1$。由于$Q(\theta)$中仅有一个基本单位数，故存在有理整数$u_1, u_2$使得

$$\varepsilon_1^{u_1} = \varepsilon_2^{u_2}。 \tag{4}$$

由于$\varepsilon_1, \varepsilon_2$均不是域$Q(\theta)$中的单位根，故若$u_2 \equiv 0 \pmod 3$，由(4)推出$u_1 \equiv 0 \pmod 3$。因此，我们可设$u_2 \not\equiv 0 \pmod 3$，于是(4)可化为

$$\varepsilon_1^u = \varepsilon_2, \tag{5}$$

其中$u = \dfrac{u_1}{u_2}$是3-adic整数。首先假设$y_1 \equiv 0 \pmod 3$，此时$x_1 \not\equiv 0 \pmod 3$，改写(5)式为

$$x_1^u\left(1 + \frac{y_1}{x_1}\theta\right)^u = \varepsilon_2,$$

展开$\left(1 + \dfrac{y_1}{x_1}\theta\right)^u$为幂级数，比较$\theta^2$的系数，注意到右边$\theta^2$的系数为0得

$$\binom{u}{2}\left(\frac{y_1}{x_1}\right)^2 + \binom{u}{5}\left(\frac{y_1}{x_1}\right)^5 d + \binom{u}{8}\left(\frac{y_1}{x_1}\right)^8 d^2 + \cdots = 0。$$

在$u \neq 0$，1时，上式中除去$2\binom{u}{2}\left(\dfrac{y_1}{x_1}\right)^2$得

$$\frac{1}{2} + \binom{u-2}{3}\frac{d}{4\cdot5}\left(\frac{y_1}{x_1}\right)^3 + \binom{u-2}{6}\frac{d^2}{7\cdot8}\left(\frac{y_1}{x_1}\right)^6 + \cdots = 0,$$

因为$y_1 \equiv 0 \pmod 3$，对此取模3知不可能。而$u = 0$，1时分别给出$\varepsilon_2 = 1$和$\varepsilon_2 = \varepsilon_1$，这些都不合假设。现在假设$y_1 \not\equiv 0 \pmod 3$，因为

$$\varepsilon_1^3 = x_1^3 + 3x_1^2 y_1\theta + 3x_1 y_1^2\theta^2 + y_1^3\theta^3$$
$$= 1 + 3x_1^2 y_1\theta + 3x_1 y_1^2\theta^2 = 1 + 3\xi,$$

故可令$u = 3v + u_0$，$u_0 = 0$，1，2，于是对(5)取模3得

$$\varepsilon_1^{u_0} \equiv \varepsilon_2 \pmod 3)。\qquad (6)$$

如果$u_0 = 2$，因为$\varepsilon_1^2 = x_1^2 + 2x_1 y_1\theta + y_1^2\theta^2$，故由(6)式比较$\theta^2$的系数推出$y_1 \equiv 0 \pmod 3$，与此时假设$y_1 \not\equiv 0 \pmod 3$矛盾。如果$u_0 = 0$，则$u = 3v$，(5)式给出

$$(1 + 3\xi)^v = x_2 + y_2\theta,$$

即

$$\sum_{t=0}^{\infty} 3^t \xi^t \binom{v}{t} = x_2 + y_2\theta,$$

由$\xi = x_1^2 y_1\theta + 3x_1 y_1^2\theta^2$知，比较上式两端$\theta^2$的系数，且令$\xi^t$中$\theta^2$的系数为$b_t$，则上式给出

$$\sum_{t=0}^{\infty} 3^t b_t \binom{v}{t} = 0,$$

即

$$3x_1 y_1^2 v + 3^2 x_1^4 y_1^2 \binom{v}{2} + \cdots = 0。$$

除去$3x_1 y_1^2$得

$$v + 3B_2\binom{v}{2} + 3^2 B_3\binom{v}{3} + \cdots = 0, \qquad (7)$$

这里$B_i(i = 2,3,\cdots)$是关于x_1, y_1的整系数多项式。如果$v \neq 0$，可设$|v|_3 = \frac{1}{3^\lambda}$，$\lambda \geqslant 0$，则由

$$3^{t-1}B_t\binom{v}{t} = 3^{t-1}\frac{vB_t}{t}\binom{v-1}{t-1}, \quad t \geqslant 2,$$

及$\frac{3^{t-2}}{t}$是一个3-adic整数知，(7)式除$|v|_3 = \frac{1}{3^\lambda}$外，其

他各项均有 $\left|3^{t-1}B_t\binom{v}{t}\right|_3=\frac{1}{3^{\lambda'}}(t\geq 2)$ 且 $\lambda'>\lambda$。故(7)式给出 $v=0$，从而 $\varepsilon_2=1$，仍不可能。

最后考虑 $u_0=1$，此时 $u=3v+1$，由(5)得

$$(x_1+y_1\theta)\sum_{t=0}^{\infty}3^t\xi^t\binom{v}{t}=x_2+y_2\theta。$$

以 b_t 和 c_t 分别表示 ξ^t 中 θ^2 和 θ 的系数，则比较上式 θ^2 的系数得

$$x_1\sum_{t=0}^{\infty}3^tb_t\binom{v}{t}+y_1\sum_{t=0}^{\infty}3^tc_t\binom{v}{t}=0。$$

除去 $3x_1^2y_1^2$ 得

$$2v+3c_1\binom{v}{2}+3^2c_2\binom{v}{3}+\cdots=0,$$

这里 $c_i(i=1,2,\cdots)$ 是关于 x_1,y_1 的整系数多项式。由此仍推出 $v=0$，从而 $u=1$，$\varepsilon_1=\varepsilon_2$，不符合假设。证毕。

由例1可推出 $x^3+(k^3-1)y^3=1$ 仅有整数解 $x=1$，$y=0$ 和 $x=k$，$y=1$。

例2 丢番图方程

$$x^3+3xy^2-3y^3=1 \tag{8}$$

仅有整数解 $(x,y)=(1,0)$ 和 $(1,1)$。

证 设 θ 满足方程 $\theta^3+3\theta-3=0$，则三次域 $Q(\theta)$ 的整底是 $1,\theta,\theta^2$，基本单位数是 $\varepsilon=1-\theta$，$N(\varepsilon)=1$，故(8)可化为 $N(x-y\theta)=1$，由此即得

$$x-y\theta=\varepsilon^u,\quad u\in Z。 \tag{9}$$

由于 $\varepsilon^3=(1-\theta)^3=1-3\theta+3\theta^2-\theta^3=1+3(\theta^2-1)$，令 $\xi=\theta^2-1$，则 $\varepsilon^3=1+3\xi$，于是在 $u\equiv 2(\bmod 3)$ 时，(9)给出

$$x-y\theta\equiv\varepsilon^2=\theta^2-2\theta+1(\bmod 3),$$

比较 θ^2 系数知 $0\equiv 1(\bmod 3)$，这不可能。因此可设 $u=3v$ 或

$u=3v+1$。

在$u=3v$时，(9)给出

$$x-y\theta=(1+3\xi)^v=\sum_{t=0}^{\infty}3^t\xi^t\binom{v}{t},\qquad(10)$$

在$u=3v+1$时，(9)给出

$$x-y\theta=(1-\theta)\sum_{t=0}^{\infty}3^t\xi^t\binom{v}{t},\qquad(11)$$

故比较θ^2系数知(10)和(11)均给出$v=0$（参见例1的处理），于是$u=0$，1，由(9)给出$x=1$，$y=0$和$x=1$，$y=1$。证毕。

利用p-adic 方法可以处理更多的二元三次式方程的整数解，例如丢番图方程

$$x^3-3xy^2-y^3=1$$

仅有整数解$(x, y)=(1, 0)$，$(0, -1)$，$(-1, 1)$，$(1, -3)$，$(-3,2)$和$(2, 1)$。有些二元三次式方程有很多的解，因此处理起来相当麻烦。例如丢番图方程

$$x^3+ax^2y-(a+1)xy^2+y^3=1$$

有解$x=1$，$y=0$；$x=0$，$y=1$；$x=1$，$y=1$；$x=1$，$y=a$；$x=-a-1$，$y=1$。当$a=3$时，除上述五组解外，还有四组解$x=-1$，$y=-2$；$x=-2$，$y=-3$；$x=9$，$y=13$和$x=-5$，$y=-14$。但我们不知道它们是否是当$a=3$时的全部解。

我们看到，p—adic 方法实际是根据代数数论知识把研究的问题化为方程(1)的形式，根据单位数的性质建立等式，然后比较素数p的方幂。因此，p-adic 方法是初等方法中比较素数幂法的进一步深化。

例3 设 $\omega=\dfrac{1+\sqrt{-7}}{2}$，$\overline{\omega}=\dfrac{1-\sqrt{-7}}{2}$，则

$$\frac{\omega^x-\overline{\omega}^x}{\omega-\overline{\omega}}=-1$$

仅有正整数解$x=3$，5和13。

证 显然$2\nmid x$，由$\dfrac{\omega^x-\overline{\omega}^x}{\omega-\overline{\omega}}=-1$展开得

$$-2^{x-1}=\binom{x}{1}-\binom{x}{3}7+\binom{x}{5}7^2+\cdots,$$

故得

$$-2^{x-1}\equiv x(\text{mod } 7),$$

此给出$x\equiv 3$，5，13(mod 42)。下面只需证明不能有$x\equiv x_1$ (mod 42)，$x_1\overline{\in}\{3,5,13\}$满足

$$\frac{\omega^x-\overline{\omega}^x}{\omega-\overline{\omega}}=\frac{\omega^{x_1}-\overline{\omega}^{x_1}}{\omega-\overline{\omega}}=-1。$$

为此设$7^\lambda\|(x-x_1)$，$\lambda>0$，则

$$\omega^x=\omega^{x_1}\omega^{x-x_1}=\omega^{x_1}\left(\frac{1}{2}\right)^{x-x_1}\left(1+\sqrt{-7}\right)^{x-x_1}$$

即

$$2^{x-x_1}\omega^x=\omega^{x_1}(1+\sqrt{-7})^{x-x_1}。\tag{12}$$

因为$x-x_1\equiv 0(\text{mod } 6)$，故

$$2^{x-x_1}\equiv 1(\text{mod } 7^{\lambda+1}),$$

而

$$(1+\sqrt{-7})^{x-x_1}=1+\binom{x-x_1}{1}\sqrt{-7}+\binom{x-x_1}{2}\left(\sqrt{-7}\right)^2$$
$$+\cdots\equiv 1+(x-x_1)\sqrt{-7}(\text{mod } 7^{\lambda+1}),$$

故(12)给出

$$\omega^x\equiv\omega^{x_1}(1+(x-x_1)\sqrt{-7})(\text{mod } 7^{\lambda+1})。$$

又

$$\omega^{x_1}\equiv\frac{1+x_1\sqrt{-7}}{2^{x_1}}(\mathrm{mod}\ 7), x-x_1\equiv 0(\mathrm{mod}\ 7^{\lambda}),$$

故得

$$\omega^{x}\equiv\omega^{x_1}+\frac{(x-x_1)\sqrt{-7}}{2^{x_1}}(\mathrm{mod}\ 7^{\lambda+1})。\tag{13}$$

同理

$$\overline{\omega}^{x}\equiv\overline{\omega}^{x_1}-\frac{(x-x_1)\sqrt{-7}}{2^{x_1}}(\mathrm{mod}\ 7^{\lambda+1})。\tag{14}$$

由(13)、(14)两式相减得

$$\omega^{x}-\overline{\omega}^{x}\equiv\omega^{x_1}-\overline{\omega}^{x_1}+2\cdot\frac{(x-x_1)\sqrt{-7}}{2^{x_1}}(\mathrm{mod} 7^{\lambda+1})。$$

由于$\omega^{x}-\overline{\omega}^{x}=\omega^{x_1}-\overline{\omega}^{x_1}$，故上式推出$7^{\lambda+1}|(x-x_1)$。这与假设$7^{\lambda}\|(x-x_1)$矛盾。于是$x=3, 5, 13$。证毕。

下面我们用p-adic 方法证明一个熟知的结果。

例4 丢番图方程

$$x^4-2y^4=1\tag{15}$$

仅有整数解$x=\pm1$, $y=0$。

证 显然，(15)给出$y\equiv0(\mathrm{mod}\ 2)$，以$2y$代$y$，(15)给出

$$x^4-32y^4=1。\tag{16}$$

由于四次域$Q(\theta)(\theta=\sqrt[4]{2})$中的基本单位是$1+\theta$和$1+\theta^2$，而(16)给出$N(x+2y\theta)=1$，故存在有理整数$u$，$v$使得

$$\pm(x+2y\theta)=(1+\theta)^{u}(1+\theta^2)^{v},\tag{17}$$

取模2得

$$x\equiv\left[1+\binom{u}{1}\theta+\binom{u}{2}\theta^2+\cdots\right]\left[1+\binom{v}{1}\theta^2+\binom{v}{2}\theta^4+\cdots\right]$$

$(\mathrm{mod}\ 2)$，由此推出$u\equiv 0(\mathrm{mod}\ 2)$。

现在展开(17)式的右端，并比较θ^2,θ^3的系数可得

$$\binom{u}{2}+v+2\left[\binom{u}{6}+\binom{u}{4}v+\binom{u}{2}\binom{v}{2}+\binom{v}{3}\right]+2^2(\cdots)$$
$$=0, \tag{18}$$

$$\binom{u}{3}+uv+2\left[\binom{u}{7}+\binom{u}{5}v+\binom{u}{3}\binom{v}{2}+u\binom{v}{3}\right]+2^2(\cdots)$$
$$=0。 \tag{19}$$

由(18)式乘u减去(19)式得

$$-\frac{(u+1)u(u-1)}{3}+2\left\{\binom{u}{7}-u\binom{u}{6}+\left[\binom{u}{5}-u\binom{u}{4}\right]v\right.$$

$$\left.+\left[\binom{u}{3}-u\binom{u}{2}\right]\binom{v}{2}\right\}+2^2(\cdots)=0。 \tag{20}$$

如果$u\neq 0$，则由于$u\equiv 0(\mathrm{mod}\ 2)$，可设$2^\lambda\|u$，$\lambda\geqslant 1$，于是由

$$\binom{u}{2n+1}=\frac{u}{2n+1}\binom{u-1}{2n}\equiv 0\ (\mathrm{mod}\ 2^\lambda)$$

知(20)推出$2^{\lambda+1}|u$，这不可能。这就证明了$u=0$，所以(18)式给出

$$v+2\binom{v}{3}+2^2\binom{v}{5}+\cdots=0,$$

与前同理，若$v\neq 0$，设$2^\lambda\|v$,则由于$2^\lambda\left|\binom{v}{2n+1}\right.$知，上式给出$2^{\lambda+1}|v$，故$v=0$。这样(17)式就给出$x=\pm 1,y=0$。证毕。

例4告诉我们怎样处理域$Q(\theta)$中有两个基本单位数的情形。

习　　题

1. 用p-adic方法证明丢番图方程$x^4-8y^4=1$仅有整数解$x=\pm1$，$y=0$。

2. 证明丢番图方程$x^3+2y^2=1$ 仅有正整数解$x=1$，$y=0$；$x=-1$，$y=\pm1$和$x=-23$，$y=\pm78$。

3. 证明丢番图方程$x^3-1=7y^2$仅有整数解$x=1$，$y=0$；$x=2$，$y=\pm1$；$x=4$，$y=\pm3$和$x=22$，$y=\pm39$。

4. 证明丢番图方程$x^3+x^2y-2xy^2-y^3=1$仅有整数解$x=1,y=0$；$x=0,y=-1$；$x=-1,y=1$；$x=-1,y=-1$；$x=2,y=-1$；$x=-1,y=2$；$x=5$，$y=4$；$x=4$，$y=-9$和$x=-9,y=5$。

5. 证明丢番图方程$x^3-4xy^2+2y^3=1$仅有整数解$x=-1$，$y=-1$；$x=1$，$y=0$；$x=1$，$y=2$；$x=-5$，$y=3$和$x=-31$，$y=14$。

（提示：设θ满足$\theta^3-4\theta+2=0$，在三次域$Q(\theta)$中，由于$Q(\theta)$的整底为1，θ，θ^2，基本单位数为$1-\theta$，$1-2\theta$，故原方程可化为$\pm(x-y\theta)=(1-\theta)^u(1-2\theta)^v$，然后用例4的方法证明仅有$u=1$，$v=0$；$u=0$，$v=1$；$u=0$，$v=0$；$u=5$，$v=-2$和$u=8$，$v=1$）。

§4　丢番图逼近方法

丢番图逼近的成果被用来求解丢番图方程是十分自然的。因为丢番图逼近的主要研究任务是确定有理数逼近一个实数的精度，因此可利用丢番图逼近的成果来证明丢番图方程的解数有限或无限，也可以定出丢番图方程解的范围，再使

用计算方法给出方程的全部整数解。

下面我们列出丢番图逼近的一些结果，这些结果都在解丢番图方程中发挥了重要作用。

Ⅰ． 有理数逼近代数数有过一些工作。一个简单的结果是Dirichlet定理：设θ是一个无理数，则有无穷多对整数x，$y>0$适合不等式

$$\left|\frac{x}{y}-\theta\right|<\frac{1}{y^2}。$$

假设θ是一个$n>1$次实的代数数，1909年Thue证明了对任给的$\varepsilon>0$，当$\mu=\frac{1}{2}n+1$时，满足不等式

$$\left|\frac{x}{y}-\theta\right|<\frac{1}{y^{\mu+\varepsilon}}。\qquad (1)$$

的整数$x,y>0$仅有有限组。后来，Siegel和Dyson又分别把(1)式中的μ改进为$\mu=\min\limits_{1\leqslant s\leqslant n-1}\left(s+\frac{n}{s+1}\right)$和$\mu=\sqrt{2n}$。显然，这些改进都与代数数$\theta$的次数有关。1955年，Roth得到了突破性的结果，他的结果与θ的次数无关。Roth[4]证明了：对任给的$\varepsilon>0$，满足不等式

$$\left|\frac{x}{y}-\theta\right|<\frac{1}{y^{2+\varepsilon}}$$

的整数x，$y>0$只有有限组。由Dirichlet定理知，Roth的这一结果已不能再改进了。Roth的这一重要结果获得了1958年国际数学家大会的菲尔兹(Fields)奖。

Ⅱ． 1966年前后，Baker[5]证明了一个十分重要的定理：设$\alpha_1,\cdots,\alpha_n$是$n>1$个非零代数数，$\alpha_i\,(i=1,\ \cdots,\ n)$的次数和高分别不超过$d\geqslant 4$和$h\geqslant 4$。如果存在整数$b_1$，$\cdots$，

b_n满足

$$0<|b_1\log\alpha_1+\cdots+b_n\log\alpha_n|<e^{-\delta H},$$

这里$0<\delta\leqslant 1$，$H=\max(|b_1|, \cdots, |b_n|)$，则

$$H<(4^{n^2}\delta^{-1}d^{2n}\log h)^{(2n+1)^2}。$$

这里所谓代数数α的次数d和高h，是指α所适合的整系数不可约多项式$a_m x^m+\cdots+a_1x+a_0(a_m\neq 0)$的次数$m$和系数$|a_j|(j=0, 1, \cdots, m)$的最大值，即$h=\max(|a_0|, |a_1|, \cdots, |a_m|)$。

利用Baker定理可以给出一类丢番图方程解的范围。对于仅有有限个解的丢番图方程，有希望给出它们解的上界。而给出了上界，便存在一个有效的计算方法给出全部解，因而使用Baker定理的方法又称为"有效方法"。Baker因为这项出色的工作，获得了1970年国际数学家大会的菲尔兹奖。

Ⅲ. 我们引进函数

$$F(\alpha,\beta,\gamma,z)=1+\frac{\alpha\cdot\beta}{1\cdot\gamma}z+\frac{\alpha(\alpha+1)\cdot\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}z^2+\cdots,$$

易知该函数右端的幂级数在$|z|<1$或$z=1$，$\gamma-\alpha-\beta>0$时是收敛的，而且它满足微分方程

$$z(z-1)F''+[(\alpha+\beta+1)z-\gamma]F'+\alpha\beta F=0。$$

设n_1, n_2是正整数，$n=n_1+n_2$，$n_2\geqslant n_1$。令

$G(z)=F(-\frac{1}{2}-n_2, -n_1, -n, z)$，$H(z)=F(\frac{1}{2}-n_1, -n_2, -n, z)$，以及

$$E(z)=\frac{F(n_2+1, n_1+\frac{1}{2}, n+2, z)}{F(n_2+1, n_1+\frac{1}{2}, n+2, 1)},$$

则Beukers[6]证明了$G(z)$和$H(z)$是次数分别为n_1，n_2的多项式，且$G(z)-H(z)\sqrt{1-z}=z^{n+1}G(1)E(z)$。从而推出

1) $|G(z)-H(z)\sqrt{1-z}|<G(1)|z|^{n+1}$, $|z|<1$;

2) $G(1)<G(z)<G(0)=1$, $0<z<1$;

3) $G(1)=\binom{n}{n_1}^{-1}\prod_{m=1}^{n_1}\left(1-\frac{1}{2m}\right)$;

4) $\binom{n}{n_1}G(z)=\sum_{k=0}^{n_1}\binom{n_2+\frac{1}{2}}{k}\binom{n-k}{n_2}(-z)^k$;

5) $\binom{n}{n_1}H(z)=\sum_{k=0}^{n_2}\binom{n_1-\frac{1}{2}}{k}\binom{n-k}{n_1}(-z)^k$;

6) 设$G^*(z)=F\Big(-\frac{1}{2}-(n_2+1),\ -(n_1+1),$

$-(n+2),\ z\Big)$,

$H^*(z)=F\Big(\frac{1}{2}-(n_1+1),\ -(n_2+1),$

$-(n+2),z\Big)$,

则有

$$G^*(z)H(z)-H^*(z)G(z)=cz^{n+1}。$$

这里$c\neq0$是常数。

利用1)～6)条可以证明丢番图逼近中的一些结果。例如1981年，Beukers[6]证明了以下定理：设$m\in Z$，则对所有整数x，均有

$$\left|\frac{x}{2^m}-\sqrt{2}\right|>2^{-1.8m-43.9}。$$

现在我们利用Ⅰ～Ⅲ来解决几种不同类型的丢番图方程。

例1 设$n\geqslant3$，$f(x,y)=a_0x^n+a_1x^{n-1}y+\cdots+a_ny^n$为不可约齐次多项式。如果$g(x,y)=\sum\limits_{r+s\leqslant n-3}b_{r,s}x^ry^s$为一次数最多为$n-3$的有理系数多项式，则丢番图方程

$$f(x,y)=g(x,y) \tag{2}$$

最多只有有限组整数解 x,y。

证 由于x,y的对称位置，不妨设$|x|\leqslant|y|$。如果$y=0$，则由$|x|\leqslant|y|=0$知$x=0$。现在可设$y>0$(因为$y<0$可将负号并入系数中去)，令$\alpha_1,\cdots,\alpha_n$为方程$f(x,1)=0$的n个根.记$G=\max\limits_{r+s\leqslant n-3}|b_{rs}|$,则由(1)式得

$$|a_0(x-\alpha_1 y)\cdots(x-\alpha_n y)|\leqslant G(1+2y+\cdots+(n-2)y^{n-2})$$
$$\leqslant n^2 G y^{n-3}, \tag{3}$$

故存在一个$j(1\leqslant j\leqslant n)$，使得

$$|x-\alpha_j y|<cy^{1-\frac{3}{n}},$$

这里$c=(n^2G/|a_0|)^{1/n}$为正常数。因为$f(x,1)$为不可约多项式，故$\alpha_1,\cdots,\alpha_n$中任两个都不同，因此对于$1\leqslant i\neq j\leqslant n$，有$|\alpha_i-\alpha_j|>c_1>0$，所以在$i\neq j$时存在正常数$c_2<c_1$，当$y>\left(\frac{c}{c_1-c_2}\right)^{\frac{n}{3}}$时有

$$|x-\alpha_i y|=|(\alpha_j-\alpha_i)y+(x-\alpha_j y)|$$
$$>c_1 y-cy^{1-\frac{3}{n}}>c_2 y,$$

故

$$\prod_{1\leqslant i\neq j\leqslant n}|x-\alpha_i y|>(c_2 y)^{n-1}。 \tag{4}$$

由(3)和(4)得出

$$|x-\alpha_j y|<\frac{c_3}{y^2}, \tag{5}$$

此处$c_3=c^n/c_2^{\,n-1}$为一正常数。现在由(5)式即得

$$\left|\frac{x}{y}-\alpha_k\right|<\frac{c_3}{y^3}<\frac{1}{y^{2+\varepsilon}},\ 1>\varepsilon>0,$$

由Ⅰ中的Roth定理知，适合此式的$x,y>0$只有有限组，这就证明了例1。证毕。

很自然地，例1中的$n=2$时结果如何？由Ⅰ中的Dirichlet定理可推出，如果方程

$$ax^2+bxy+cy^2+dx+ey+f=0$$

有解，则必有无穷多组解（这里，$b^2-4ac>0$且为非平方数）。

在例1中，利用Baker的有效方法，可以定出解的上界，参阅第八章。

例2 设Pell方程$x^2-Dy^2=1$和$x^2-D_1y^2=1$的基本解分别为$\beta=x_0+y_0\sqrt{D}$和$\beta_1=x_1+y_1\sqrt{D_1}$，则Pell方程组

$$x^2-Dy^2=1,\quad y^2-D_1z^2=1 \tag{6}$$

的整数解满足

$$|y|<M^{2^{1470}N^{49}}$$

这里$M=\max(\beta,\ \beta_1)$，$N=\log\ \max(2x_0,2x_1,D)$。

证 我们用Ⅱ中的Baker定理来证明。设x,y,z是(6)的整数解，则有

$$|y|=\frac{\beta^n-\overline{\beta}^n}{2\sqrt{D}}=\frac{\beta_1^m+\overline{\beta}_1^m}{2},m\geqslant 0,\quad n\geqslant 0, \tag{7}$$

这里$\overline{\beta}=x_0-y_0\sqrt{D}$，$\overline{\beta}_1=x_1-y_1\sqrt{D_1}$且$\beta\overline{\beta}=\beta_1\overline{\beta}_1=1$。令

$$P=\frac{\beta^n}{2\sqrt{D}},\qquad Q=\frac{\beta_1^m}{2},$$

则$P^{-1}=2\sqrt{D}\,\overline{\beta}^n$，$Q^{-1}=2\overline{\beta}_1^m$。于是(7)给出

$$P-P^{-1}\cdot\frac{1}{4D}=Q+Q^{-1}\cdot\frac{1}{4}。 \tag{8}$$

因为$P^{-1}>0$，$Q^{-1}>0$，故(8)给出$P>Q$，从而$P^{-1}<Q^{-1}$，于是由$Q^{-1}<1$知

$$P=P^{-1}\cdot\frac{1}{4D}+Q+Q^{-1}\cdot\frac{1}{4}<Q^{-1}\cdot\frac{1}{4D}+Q+Q^{-1}\cdot\frac{1}{4}$$

$$=Q+Q^{-1}\cdot\frac{D+1}{4D}<Q+\frac{D+1}{4D},$$

故

$$Q>P-\frac{D+1}{4D}。\tag{9}$$

另一方面，假设$n\geqslant3$，则

$$P=\frac{\beta^n}{2\sqrt{D}}\geqslant\frac{(1+\sqrt{D})^3}{2\sqrt{D}}=\frac{1}{2\sqrt{D}}+\frac{3}{2}+\frac{3}{2}\sqrt{D}+\frac{D}{2}$$

$$>\frac{1}{2}\left(\frac{1}{\sqrt{D}}+1\right)+\frac{D}{2}\left(\frac{1}{\sqrt{D}}+1\right)$$

$$=\frac{D+1}{2}\left(\frac{1}{\sqrt{D}}+1\right)>\frac{D+1}{2}\cdot\frac{D+1}{4D}。\tag{10}$$

因此由(9)和(10)得出

$$Q^{-1}<\left(P-\frac{D+1}{4D}\right)^{-1}<P^{-1}\cdot\frac{D+1}{D-1}。\tag{11}$$

再从(8)和(11)知

$$P-Q=P^{-1}\cdot\frac{1}{4D}+Q^{-1}\cdot\frac{1}{4}<P^{-1}\cdot\left(\frac{1}{4D}+\frac{D+1}{4(D-1)}\right)。$$

因此，当 $j\geqslant3$时

$$\frac{(P-Q)^j}{jP^j}<\frac{(P-Q)^2}{2^{j-1}P^2}。$$

现在

$$0<\log\frac{P}{Q}=\log\frac{1}{1-\frac{P-Q}{P}}$$

$$=\frac{P-Q}{P}+\frac{(P-Q)^2}{2P^2}+\sum_{j=3}^{\infty}\frac{(P-Q)^j}{jP^j}$$

$$<\frac{P-Q}{P}+\frac{(P-Q)^2}{2P^2}\sum_{j=1}^{\infty}\frac{1}{2^{j-1}}$$

$$=\frac{P-Q}{P}+\frac{(P-Q)^2}{P^2}$$

$$<P^{-2}\cdot\left(\frac{1}{4D}+\frac{D+1}{4(D-1)}\right)+P^{-4}\cdot\left(\frac{1}{4D}+\frac{D+1}{4(D-1)}\right)^2$$

$$<P^{-2}\cdot\left(\frac{1}{4D}+\frac{D+1}{4(D-1)}\right)\left[1+\frac{16D(D^2+2D-1)}{(D-1)(D+1)^4}\right]。$$

故把$P=\frac{\beta^n}{2\sqrt{D}}$，$Q=\frac{\beta_1{}^m}{2}$代入上式得

$$0<n\log\beta-\log\sqrt{D}-m\log\beta_1$$

$$<D\left(\frac{1}{D}+\frac{D+1}{D-1}\right)\left[1+\frac{16D(D^2+2D-1)}{(D-1)(D+1)^4}\right]\beta^{-2n}。\quad(12)$$

如果$n\geqslant m$，则(12)式右端$<e^{-n}$，故由Ⅱ中的Baker定理知

$$n\leqslant[4^9\cdot4^6\log\ \max(2x_0,2x_1,D)]^{49}$$

$$=2^{1470}N^{49}。$$

如果$n<m$，则由$P>Q$，我们有

$$D\beta^{-2n}<\beta_1{}^{-2m},$$

因此(12)式右端$<e^{-m}$，故由Baker定理知

$$m<2^{1470}N^{49}。$$

于是，从(7)式知

$$|y|<(\max(\beta,\beta_1))^{\max(m,n)}$$
$$<M^{2^{1470}}\cdot N^{49}$$

证毕。

由例2知，Pell方程组(6)最多仅有有限组整数解。对于某些给定值的D,D_1，利用Baker的有效方法加上一些计算可以给出(6)的全部整数解。

例3 Pell方程组

$$x^2-2y^2=1,\qquad y^2-3z^2=1 \tag{13}$$

仅有整数解$x=\pm3$，$y=\pm2$，$z=\pm1$。

证 由于(13)式中两个Pell方程基本解分别为

$\beta=3+2\sqrt{2}$，$\beta_1=2+\sqrt{3}$，故由例2知

$$|y|<(3+2\sqrt{2})^{2^{1470}\cdot(\log 6)^{49}}<5^{10^{460}}。$$

这个界虽然很大，但Grinetead[7]提出了一个用计算机处理的办法。由(13)解出

$$|y|=\frac{\beta^n-\bar\beta^n}{2\sqrt{2}}=\frac{\beta_1^m+\bar\beta_1^m}{2},\quad m\geqslant0,\quad n\geqslant0, \tag{14}$$

假设(14)式成立，则Grinetead验证了小于1095的所有素数p，发现(14)均给出$n\equiv1(\bmod\ p)$，于是

$$n\equiv1(\bmod \prod_{p<1095}p)。$$

由此知$n=1$或$n>\prod\limits_{p<1095}p$，但由于

$$\prod_{p<1095}p>10^{460},$$

故在$n>\prod\limits_{p<1095}p$时(14)给出

$$|y|>5^{10^{460}},$$

因此只能$n=1$，从而$|y|=\dfrac{\beta-\bar\beta}{2\sqrt{2}}=2$，于是给出(13)仅有

整数解$x=\pm 3$，$y=\pm 2$，$z=\pm 1$。证毕

例4 设$D\neq 0\in Z$，如果丢番图方程

$$x^2-D=2^n \tag{15}$$

有正整数解，则$n<435+\dfrac{10\log|D|}{\log 2}$。

证 如果n为偶数，则(15)给出

$$|D|=|x^2-2^n|=|x-2^{n/2}|\cdot|x+2^{n/2}|>2^{n/2},$$

故$n<\dfrac{2\log|D|}{\log 2}$，即结论成立。

现设$2\nmid n$，$n=2m+1$，则由Ⅲ中Beukers定理知

$$\left|\frac{x}{2^m}-\sqrt{2}\right|>2^{-1.8m-43.9},$$

故

$$\left|\frac{x}{2^{n/2}}-1\right|>2^{-0.9n-43.5}。\tag{16}$$

现由(15)式推出$\left|\dfrac{x}{2^{n/2}}-1\right|<|D|2^{-n}$，故结合(16)式得出

$n<435+\dfrac{10\log|D|}{\log 2}$。证毕。

最后指出，利用Ⅰ～Ⅲ中的结果可以给出许多著名问题的解答。对于Ⅲ，由于从1)～6)可以推出一系列丢番图不等式，故可用来解更为广泛的丢番图方程。

习　题

1．利用Thue定理证明：设$n\geqslant 3$，$f(x,y)$是n次不可约的齐次多项式，则$f(x,y)=a$(a为常数)仅有有限组解。

2．利用Roth定理证明：设p,q是不同的奇素数，则在$p>2(q-1)$或$q>2(p-1)$时，Catalan方程

$$x^p-y^q=1$$

最多仅有有限组整数解x,y。

3．如果丢番图方程$y^2=x^3+k, k\neq 0$有整数解x,y，则必有$\max(|x|,|y|)\leqslant\exp(10^{10}|k|^{10^4})$

4．利用Beukers定理，证明丢番图方程$x^2+7=2^n$仅有正整数解$(x,n)=(1,3),(3,4),(5,5),(11,7),(181,15)$。

5．设q是一个素数幂，$2\nmid m\geqslant 5$。如果丢番图方程$x^2=4q^m+4q^2+1$有整数解，则$q<40$。

§5 其他的一些高等方法

本节我们介绍解析数论和丢番图几何的成果在解一些丢番图方程时的应用。我们知道，解析数论和丢番图几何的成果异常丰富，它们研究的对象都是丢番图方程，只是解析数论研究丢番图方程解的个数的估计，而丢番图几何研究丢番图方程上解的定性或定量性质。这一节，我们不可能涉及这两个重要分支的较为全部的结果，我们只想说明一下，这两个分支中的一些结果（有些结果直接就是关于丢番图方程的）可以给出丢番图问题的一些解答。

在解析数论中，我们熟知筛法中的一个结果：[8]设m是自然数，a_i,b_i满足$(a_i,b_i)=1(i=1,\cdots,m)$。又设$E=\prod_{i=1}^{m}a_i\prod_{1\leqslant r<s\leqslant m}(a_rb_s-a_sb_r)\neq 0$，$1<y\leqslant x$（$x,y$均为实数）。如果$P$是某些素数的集合，且有$\delta>0, A>0$使得

$$\sum_{\substack{p<y\\ p\in P}}\frac{1}{p}\geqslant\delta\log\log y-A,$$

则有

$$\#\{n: x-y<n\leqslant x, (a_i n+b_i, P)=1(i=1,\cdots,m)\}\ll$$

$$\prod_{\substack{p\mid L\\ p\in P}}\left(1-\frac{1}{p}\right)^{\rho(p)-m}\cdot\frac{y}{(\log y)^{\delta m}} \tag{1}$$

且包含在≪中的常数仅与m和A有关。其中$\rho(p)$表示$\prod_{i=1}^{m}(a_i n+b_i)\equiv 0(\bmod p)$的解数，而$(a_i n+b_i, P)=1$表示$a_i n+b_i$与$P$中的每一素数互素，而#{ }表示集合{ }中的元素个数。

利用这个结果，我们来证明

例1 设$S(N)$表示不超过N使方程

$$\frac{4}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \tag{2}$$

没有正整数解的那些n的个数，则有

$$S(N)\ll\frac{N}{(\log N)^2}。$$

证 容易验证，当$n=(4k-1)v$时有

$$\frac{4}{n}=\frac{1}{kv}+\frac{1}{n(k+1)}+\frac{1}{nk(k+1)};$$

当$n+1=(4k-1)v$时有

$$\frac{4}{n}=\frac{1}{kv}+\frac{1}{nk}+\frac{1}{nkv};$$

当$n+4=(4k-1)v$时有

$$\frac{4}{n}=\frac{1}{kv-1}+\frac{1}{nk}+\frac{1}{nk(kv-1)};$$

当$4n+1=(4k-1)v$时有

$$\frac{4}{n}=\frac{1}{nk}+\frac{1}{k(kv-n)}+\frac{1}{n(kv-n)};$$

故取

$$P=\{p: p\equiv -1(\bmod\ 4)\},\ y=x,\ m=4,$$

$$\prod_{i=1}^{4}(a_i n+b_i)=n(n+1)(n+4)(4n+1),$$

得$E=4\cdot 3^3\cdot 5\neq 0$，$\rho(3)=2$，$\prod_{\substack{p\mid E\\ p\in P}}\left(1-\frac{1}{p}\right)^{\rho(p)-m}$

$$=\left(\frac{2}{3}\right)^{-2}。$$

由Mertens的结果（看[8]）知

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{1}{p}=\frac{1}{\varphi(k)}\log\log x+O_k(1),\ (l,\ k)=1,$$

故取$k=4$，$l=-1$，知

$$\sum_{\substack{p\leqslant x\\ p\in P}}\frac{1}{p}\geqslant\frac{1}{2}\log\log x-A,$$

所以可取$\delta=\frac{1}{2}$，由(1)得出

$$S(x)\ll\frac{x}{(\log x)^2}。$$ 证毕。

Erdös曾经猜测，对大于1的每个正整数n，方程(2)均有正整数解。而例1的结论说明，对“几乎所有”的n，Erdös的这个猜测都成立。例1的这个十分简短的证明是杨训乾[9]

得到的，对于这个问题的进一步推广，即对于方程

$$\sum_{i=0}^{k}\frac{1}{x_i}=\frac{a}{n}，a\text{是给定的正整数，} \tag{3}$$

设$E_{a,k}(N)$表示不超过N使(3)没有正整数解的那些n的个数，则单墫[10]用解析数论的方法证明了

$$E_{a,k}(N)\ll N\exp\left(-c(\log N)^{1-\frac{1}{k+1}}\right)。$$

且包含在$\ll$中的常数依赖于a和k。

例2．Catalan 方程

$$x^m-y^n=1，m>1，n>1 \tag{4}$$

在$m\geqslant 2\sqrt{xy}$，$n\geqslant 2\sqrt{xy}$时无正整数解。

证　由于方程(4)在$2|mn$时仅有正整数解$m=2$，$x=3$，$n=3$，$y=2$（参见Mordell的书[11]或第八章§3），故例2的结论成立。现在设$2\nmid mn$，由方程(4)整理得

$$\left(x^m+y^n\right)^2-xy\left(2x^{\frac{m-1}{2}}y^{\frac{n-1}{2}}\right)^2=1。 \tag{5}$$

显然$xy>0$且不是平方数。设Pell方程$\xi^2-xy\eta^2=1$的基本解为$\varepsilon=\xi_0+\eta_0\sqrt{xy}$，则(5)式给出

$$x^m+y^n=\frac{\varepsilon^k+\bar{\varepsilon}^k}{2}=2x^m-1=2y^n+1, \tag{6}$$

和

$$2x^{\frac{m-1}{2}}y^{\frac{n-1}{2}}=\frac{\varepsilon^k-\bar{\varepsilon}^k}{2\sqrt{xy}}，k>0。 \tag{7}$$

如果$2|k$，则由(6)得

$$2x^m-1=2\left(\frac{\varepsilon^{k/2}+\bar{\varepsilon}^{k/2}}{2}\right)^2-1,$$

这给出$x=x_1^2$，，$\dfrac{\varepsilon^{k/2}+\bar{\varepsilon}^{k/2}}{2}=x_1^m$。代入(7)式可得

$$x_1^{m-1}y^{\frac{n-1}{2}}=x_1^m\cdot\frac{\varepsilon^{k/2}-\bar{\varepsilon}^{k/2}}{2\sqrt{xy}},$$

此给出$x_1|y^{\frac{n-1}{2}}$。由于$(x_1,y)=1$，故$x_1=1$，从而$x=1$，$y=0$，非方程(4)的正整数解。

如果$2\nmid k$，$k>1$，可设$p|k$，p为k的任一个奇素数因子。令$k=pl$，$a_l+b_l\sqrt{xy}=\varepsilon^l$，则(7)式给出

$$2x^{\frac{m-1}{2}}y^{\frac{n-1}{2}}=\frac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{\varepsilon^l-\bar{\varepsilon}^l}\cdot\frac{\varepsilon^l-\bar{\varepsilon}^l}{2\sqrt{xy}}$$

$$=\frac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{\varepsilon^l-\bar{\varepsilon}^l}\cdot b_l。\qquad (8)$$

如果$p\nmid xy$，则$\left(\dfrac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{\varepsilon^l-\bar{\varepsilon}^l},\ xy\right)=1$且

$2\nmid\dfrac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{\varepsilon^l-\bar{\varepsilon}^l}$，故(8)给出，

$$\frac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{\varepsilon^l-\bar{\varepsilon}^l}=1,$$

而这显然不可能。

现在考虑$p|xy$。此时，在$p>3$时有$p\left\|\dfrac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{\varepsilon^l-\bar{\varepsilon}^l}\right.$，

$\dfrac{(\varepsilon^l)^p-(\bar{\varepsilon}^l)^p}{p(\varepsilon^l-\bar{\varepsilon}^l)}\equiv1\pmod{2xy}$，所以(8)给出

$$\frac{(\varepsilon^{l})^{p}-(\bar{\varepsilon}^{l})^{p}}{\varepsilon^{l}-\bar{\varepsilon}^{l}}=p,$$

此仍不可能。而对于$p=3$，可设$3\nmid b_l$，$3\mid xy$，且(8)式可化为

$$2x^{\frac{m-1}{2}}y^{\frac{n-1}{2}}=(3a_l^2+b_l^2xy)b_l, \qquad (9)$$

由$a_l^2-xyb_l^2=1$，设$3^{\alpha}\parallel x$或$3^{\alpha}\parallel y$，$\alpha\geqslant1$，则(9)给出$3a_l^2+b_l^2xy=3^{\lambda}$，$\lambda=\alpha\cdot\frac{m-1}{2}$或$\alpha\cdot\frac{n-1}{2}$，故知

$$4a_l^2-1=3^{\lambda},$$

由此得$a_l=1$，所以$l=0$。但由$l=0$代入(9)式知$xy=0$，与$xy>0$矛盾。

以上证明了$k>1$时(6)和(7)不成立。所以，

$$x^m+y^n+2x^{\frac{m-1}{2}}y^{\frac{n-1}{2}}\sqrt{xy}=\xi_0+\eta_0\sqrt{xy}。 \qquad (10)$$

现由解析数论中的Schur定理（参见[12]）知

$$\xi_0+\eta_0\sqrt{xy}<(xy)^{\sqrt{xy}},$$

故由(10)式知

$$x^m+y^n+2x^{\frac{m}{2}}y^{\frac{n}{2}}<(xy)^{\sqrt{xy}},$$

因此，设$\lambda=\min(m,n)$，可有

$$(xy)^{\frac{\lambda}{2}}<x^{\frac{m}{2}}y^{\frac{n}{2}}<x^m+y^n+2x^{\frac{m}{2}}y^{\frac{n}{2}}<(xy)^{\sqrt{xy}},$$

即$\lambda<2\sqrt{xy}$，这与$m\geqslant2\sqrt{xy}$，$n\geqslant2\sqrt{xy}$矛盾。证毕。

这个例子的证明，只用到了解析数论中的Schur定理和Pell方程方法，但收到了意想不到的结果。另外，从这个证明可见，对给定的正整数a，b，方程

$$a^x - b^y = 1, x>1, y>1$$

的解最多只有一组，且x,y中必有一个小于$2\sqrt{ab}$。

例2 所示的方法是属于曹珍富的。其一般步骤是：

1） 把欲求解的方程化为Pell方程；

2） 利用Pell方程的解的性质，把欲求解的方程化为与Pell方程基本解间的关系；

3） 利用解析数论中关于基本解的估计定出解的不等关系或解的上界。

利用这种方法，曹珍富[13]还求解了方程

$$\frac{x^m - 1}{x - 1} = y^n,\quad m>2,\quad n>1。$$

解析数论在解丢番图方程中的应用还有许多例子。1985年，Adleman和Heath-Brown[14]证明了有无穷多个素数p使Fermat大定理第一情形成立，即他们证明了：设p是奇素数，$s(N)$表示不超过N使方程$x^p + y^p = z^p$没有$p\nmid xyz$的整数解的那些p的个数，则$s(N) \gg N^{0.6687}$。后来，Heath-Brown[15]对一般的Fermat方程

$$x^n + y^n = z^n,\quad n \geqslant 3, \tag{11}$$

证明了对“几乎所有”的n，方程(11)均无整数解。设$H(N)$是不超过N使方程(11)有整数解的那些n的个数，则Heath-Brown证明了$H(N) = o(N)$（当$N \to \infty$），即对任给的$\varepsilon>0$，存在N_ε，当$N \geqslant N_\varepsilon$时$H(N) \leqslant \varepsilon N$。

Heath-Brown的这些重要结果都是基于Faltings关于丢番图几何的一个重要结果。1983年，Faltings[16]证明了著名的Mordell猜想，即“亏格”大于或等于2的有理曲线上最多仅有有限个有理点。设$f(x,y) = x^n + y^n - 1$，则$f(x,y)$的亏

格$g=\frac{(n-1)(n-2)}{2}$，故由Faltings的结果可推出，在$n\geqslant 4$时，$x^n+y^n=1$最多仅有有限个有理解。于是推出方程(11)如果有解（不妨设$(x,\ y)=1$），则仅有有限组。这是对Fermat猜想的重大突破。

由于介绍丢番图几何的成果需要其它许多专门的知识，这超出了本书的范围。有兴趣的读者可参阅Lang的书[17]。

参 考 文 献

[1] 曹珍富，自然杂志，9(1986)，720。

[2] 曹珍富，The Diophantine equation $\frac{p^x-1}{p-1}=q^y$，数学研究与评论（待发表））。

[3] 曹珍富，王笃正，科学通报，14(1987)，1043—1046。

[4] Cassels,J.W.S.,An introduction to Diophantine Approximation,Camb.Univ.Press,1957,或[12],533—548页.

[5] Baker,A., Mathematika,15(1968),204—216.

[6] Beukers,F.,Acta Arithmetica,38(1981),389—410.

[7] Grinetead, Math.Comp.,32(1978),936—940.

[8] Halberstem, H.and Richert, H.F., Siere Methods, Academic Press, 1974.

[9] 杨训乾，四川大学学报（自然科学版），3(1981)，101—103。

[10] 单墫，数学年刊，B辑，2(1986)，213—220。

[11] Mordell, L.J.,Diophantine equations, Academic Press, London and New York,1969, 301—304.

[12] 华罗庚,数论导引，第十二章,科学出版社，北京，1979，363。

[13] 曹珍富,关于丢番图方程$\frac{x^m-1}{x-1}=y^n$,在1988年9月山东大学纪念闵嗣鹤教授学术报告会上的报告。

[14] Adleman, L.M.and Heath-Brown, D. R., Invent.Math.,79(1985), 409—416.

[15] Heath-Brown, D.R.,Bull. London Math. Soc.,17(1985),15—16. MR86a：11011.

[16] Faltings, G., Invent. Math.,73(1983),349—366.

[17] Lang, S., Fundamentals of Diphantine Geometry, Springer—Verlag, 1983.

第四章　一次丢番图方程

在前面我们全面地介绍了解丢番图方程的方法。从本章开始，我们将利用这些方法介绍各种不同类型的丢番图方程的解法和结果。并且对与丢番图方程有关的问题也尽量给以阐述。

一次丢番图方程是最基本的。本章将从二元、三元的一次丢番图方程入手，导出一般的一次丢番图方程的不同解法，最后给出整系数线性型的Frobenius问题的研究情况。

§1 二元、三元的一次丢番图方程

设$s\geqslant 2$，s元一次丢番图方程是指

$$a_1x_1+\cdots+a_sx_s=n,$$

这里$a_i\neq 0(i=1,\cdots,s)$和n都是给定的整数。本节我们给出$s=2$和$s=3$的全部整数解表达式。

定理1　如果二元一次丢番图方程

$$a_1x_1+a_2x_2=n, \tag{1}$$

有整数解$x_1^{(0)}$，$x_2^{(0)}$，则(1)的全部整数解可表为

$$x_1=x_1^{(0)}+\frac{a_2}{d}t,\quad x_2=x_2^{(0)}-\frac{a_1}{d}t,\ t\in Z, \tag{2}$$

这里$d=(a_1,\ a_2)$。

证　把(2)代入(1)验证知，如果$x_1^{(0)}$，$x_2^{(0)}$是(1)的解，

则(2)式对任意$t\in Z$均是(1)的解。

现设x_1，x_2为(1)的一组整数解，我们来证明它必能表为(2)的形状。由

$$a_1x_1+a_2x_2=a_1x_1^{(0)}+a_2x_2^{(0)}=n$$

可得

$$a_1(x_1-x_1^{(0)})+a_2(x_2-x_2^{(0)})=0。\qquad (3)$$

由于$\left(\frac{a_1}{d},\ \frac{a_2}{d}\right)=1$，故(3)式给出$\frac{a_2}{d}\Big| x_1-x_1^{(0)}$，可设$x_1-x_1^{(0)}=\frac{a_2}{d}t$，$t\in Z$，于是(3)给出

$$x_1=x_1^{(0)}+\frac{a_2}{d}t,\quad x_2=x_2^{(0)}-\frac{a_1}{d}t,\quad t\in Z。$$证毕。

现在我们给出(1) 有整数解的充要条件。这样就彻底解决了方程(1)。

定理2 方程(1)有整数解的充要条件是$(a_1,a_2)|n$。

证 方程(1)有整数解显然给出$(a_1,\ a_2)|n$。现设$(a_1,\ a_2)|n$，我们来证明方程(1)必有整数解。此时不失一般可设$(a_1,\ a_2)=1$，$a_1>0$，如$a_1=1$，则(1)显然有解$x_1=n-a_2x_2$。如$a_1>1$，则可设$a_2=k_1a_1+r_1$，$0<r_1<a_1$，$(r_1,\ a_1)=1$，(1)给出

$$x_1=-k_1x_2+\frac{-r_1x_2+n}{a_1}=-k_1x_2+x_3,$$

这里$a_1x_3+r_1x_2=n$，$(r_1,\ a_1)=1$。由此可知，对于

$$a_1=k_2r_1+r_2,\quad 0<r_2<r_1,\quad (r_2,\ r_1)=1,$$
$$r_1=k_3r_2+r_3,\quad 0<r_3<r_2,\quad (r_2,\ r_3)=1,$$
$$\cdots\cdots\cdots\cdots$$
$$r_{s-1}=k_{s+1}r_s+r_{s+1},\quad r_{s+1}=0,\quad r_s=1。$$

分别得出

$$x_2 = -k_2 x_3 + x_4,\quad r_1 x_4 + r_2 x_3 = n,$$

$$x_3 = -k_3 x_4 + x_5,\quad r_2 x_5 + r_3 x_4 = n,$$

$$\cdots\cdots$$

$$x_s = -k_s x_{s+1} + x_{s+2},\quad r_{s-1} x_{s+2} + r_s x_{s+1} = n。$$

由于$r_s = 1$，后一式解出含有参数x_{s+2}（令$x_{s+2} = t$）的x_s，x_{s+1}，不断回代，最后得出方程(1)含参数t的解。证毕。

定理2的证明是构造性的，它告诉我们在方程（1)有解时怎样求其全部解。

对于三元一次丢番图方程

$$a_1 x_1 + a_2 x_2 + a_3 x_3 = n, \tag{4}$$

结果如何呢？我们在下节将证明(4)有解的充要条件是$(a_1, a_2, a_3) | n$。而在$(a_1, a_2, a_3) | n$时(4)的解可由(1)的解推出。我们有

定理3 设$(a_1, a_2, a_3) = 1$，$(a_1, a_2) = d$，则方程(4)的全部解可表为

$$x_1 = x_1^{(0)} + \frac{a_2}{d} t_1 - u_1 a_3 t_2,$$

$$x_2 = x_2^{(0)} - \frac{a_1}{d} t_1 - u_2 a_3 t_2, x_3 = x_3^{(0)} + d t_2, t_1, t_2 \in Z \tag{5}$$

其中$x_1^{(0)}$，$x_2^{(0)}$，$x_3^{(0)}$是方程(4)的任一组解，u_1，u_2满足方程$\frac{a_1}{d} u_1 + \frac{a_2}{d} u_2 = 1$。

证 经验证知，只需证明(4)的全部解可表为(5)。设x_1，x_2，x_3是(4)的任一组解，由

$$a_1 x_1^{(0)} + a_2 x_2^{(0)} + a_3 x_3^{(0)} = a_1 x_1 + a_2 x_2 + a_3 x_3 = n$$

可得

$$a_1(x_1-x_1^{(0)})+a_2(x_2-x_2^{(0)})=-a_3(x_3-x_3^{(0)}),\quad (6)$$

由$(a_1, a_2)=d$及$(d,a_3)=1$知$d\mid x_3-x_3^{(0)}$，故有整数t_2使得$x_3-x_3^{(0)}=dt_2$，代入(6)式得

$$\frac{a_1}{d}(x_1-x_1^{(0)})+\frac{a_2}{d}(x_2-x_2^{(0)})=-a_3t_2 \quad (7)$$

根据$\frac{a_1}{d}u_1+\frac{a_2}{d}u_2=1$ 知，方程$\frac{a_1}{d}u+\frac{a_2}{d}v=-a_3t_2$ 有一组解$u=-u_1a_3t_2$，$v=-u_2a_3t_2$，故由定理1,(7)的全部解可表为

$x_1-x_1^{(0)}=-u_1a_3t_2+\frac{a_2}{d}t_1$，$x_2-x_2^{(0)}=-u_2a_3t_2-\frac{a_1}{d}t_1$，

这里$t_1\in Z$。这就得出(4)的解均可表为(5)的形状。证毕。

§2　$s\geqslant 2$元一次丢番图方程

很自然地，二元、三元一次丢番图方程的结果是否可推广到一般的$s\geqslant 2$元一次丢番图方程

$$a_1x_1+\cdots+a_sx_s=n \quad (1)$$

上去？这里$a_i\neq 0(i=1,\cdots,s)$和n都是给定的整数。我们将证明一些类似的结果。

定理1　方程(1)有解的充要条件是$(a_1,\cdots,a_s)\mid n$。

证　如(1)有解，显然有$(a_1,\cdots,a_s)\mid n$。现设$(a_1,\cdots,a_s)\mid n$，来证明方程(1)有解。设$(a_1,\cdots,a_s)=d_s$，首先对$s\geqslant 2$用归纳法证明必存在整数$y_1,\cdots y_s$使得

$$a_1y_1+\cdots+a_sy_s=d_s。\quad (2)$$

$s=2$时结论显然成立(见§1的定理1)，设s时结论成立，则在$s+1$时，有

$$d_{s+1}=(a_1,\cdots,a_s,\ a_{s+1})=(d_s,a_{s+1})$$
$$=d_s\lambda+a_{s+1}y_{s+1}=a_1(\lambda y_1)+\cdots+a_s(\lambda y_s)$$
$$+a_{s+1}y_{s+1}。$$

这就证明了(2)式成立。于是，在 $d_s|n$ 时，在(2)两端乘以 $\frac{n}{d_s}$，得出

$$a_1\left(\frac{n}{d_s}y_1\right)+\cdots+a_s\left(\frac{n}{d_s}y_s\right)=n,$$

即方程(1)有解 $x_i=\frac{n}{d_s}y_i(i=1,\cdots,s)$。证毕。

现在的问题是，方程(1) 有解时，怎样求出全部解？正如三元的情形一样，它也可以化为若干二元的情形来解决。设$(a_1,\ a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{s-1},a_s)=d_s(=d)$，则方程(1)可化为

$$a_1x_1+a_2x_2=d_2y_2,$$
$$d_2y_2+a_3x_3=d_3y_3,$$
$$\cdots\cdots$$
$$d_{s-2}y_{s-2}+a_{s-1}x_{s-1}=d_{s-1}y_{s-1},$$
$$d_{s-1}y_{s-1}+a_sx_s=n。$$

然后由后一式解出y_{s-1}，x_s，将y_{s-1}代入上一式解出y_{s-2}，x_{s-1}，再将y_{s-2}代入上式，不断做下去，直至解出x_1,x_2。这样便得出方程(1) 的全部解，而且由于每解一个二元一次丢番图方程增加一个整数参数，故方程(1) 的全部解中一定含有$s-1$个整数参数。

除开这种逐次求出方程(1) 的全部解外，是否存在一个表达式，给出方程(1)的全部解？1984年，徐肇玉和曹珍富[1]证明了

定理2 设$x_1=x_1^{(0)}$，…，$x_s=x_s^{(0)}$是方程（1)的任一组整数解,则存在$t(1\leqslant t\leqslant s)$使得方程(1)的全部整数解可表为

$$x_i=x_i^{(0)}+D\frac{m_i}{n_i}[n_1,\cdots,n_{t-1},\ n_{t+1},\cdots,n_s]$$

$$(i=1,\cdots,s),\quad D\in Z, \tag{3}$$

其中m_i，$n_i\in Z(1\leqslant i\leqslant s)$满足以下条件：

1) $(m_i,n_i)=1$，$n_i\neq 0\quad(i=1,\cdots,s)$；

2) $\frac{m_t}{n_t}=1$且$\frac{m_{t-1}}{n_{t-1}}=-\frac{1}{a_{t-1}}\sum\limits_{\substack{1\leqslant i\leqslant s\\ i\neq t-1}}a_i\frac{m_i}{n_i}$。

这里约定$t=1$时$m_{t-1}=m_s$，$n_{t-1}=n_s$。

证 容易验证，(3)确为(1)的解。现证(1)的任一解均可表为(3)。为此，令$x_i=x_i^{(0)}+y_i(i=1,\cdots,s)$代入方程(1)得

$$a_1y_1+\cdots+a_sy_s=0。\tag{4}$$

设$y_i=Dz_i(i=1,\cdots,s)$，$D\in Z$且$(z_1,\cdots,z_s)=1$。在$D=0$时，显然推出(3)；在$D\neq 0$时，(4)化为

$$a_1z_1+\cdots+a_sz_s=0,\ (z_1,\cdots,z_s)=1。\tag{5}$$

由(5)知，必存在$t(1\leqslant t\leqslant s)$，$z_t\neq 0$。于是可取$\frac{z_i}{z_t}=\frac{m_i}{n_i}$，$(m_i,n_i)=1$且$n_i\neq 0(i=1,\cdots,s)$，满足$\sum\limits_{i=1}^{s}a_i\frac{m_i}{n_i}=0$。由$(z_1,\cdots,z_s)=1$知$z_t=[n_1,\cdots,n_{t-1},\ n_{t+1},\ \cdots,\ n_s]$。于是由$x_i=x_i^{(0)}+y_i=x_i^{(0)}+Dz_i=x_i^{(0)}+D\frac{m_i}{n_i}z_t$即知，方程(1)推出(3)。证毕。

由定理2可以十分方便地求出方程(1)含一个参数的解，例如对方程

$$2x_1+5x_2+7x_3+3x_4=10, \tag{6}$$

显然它有一组解(5,0,0,0)。如取$\frac{m_1}{n_1}=\frac{5}{6}$，$\frac{m_2}{n_2}=\frac{3}{4}$，则

$$\frac{m_3}{n_3}=-\frac{1}{7}\left(\frac{2\cdot5}{6}+\frac{5\cdot3}{4}+3\right)=-\frac{101}{84},$$ 而$(6,5)=(4,3)=(84,-101)=1$，$[6,4,84]=84$，故(6)有整数解$x_1=5+70D$，$x_2=63D$，$x_3=101D$，$x_4=84D$，$D\in Z$。

1985年，凌露娜[2]利用整数矩阵的初等变换给出了一个求方程(1)解的方法。所谓整数矩阵的初等变换是指：

1） 非零整数乘矩阵的某一行；

2） 矩阵的某一行乘以$c\in Z$，加到另一行；

3） 矩阵中的两行互换。

现在给出利用2)和3)的初等变换求解方程(1)的结果。首先将方程(1)的s个系数排成一列，在这列的右边添加一个s阶单位矩阵，得到一个$s\times(s+1)$的整数矩阵

$$A=\begin{pmatrix} a_1 & 1 & 0\cdots & 0 \\ a_2 & 0 & 1\cdots & 0 \\ \cdots & \cdots & & \cdots \\ a_s & 0 & 0\cdots & 1 \end{pmatrix},$$

然后对A施行2)和3)的初等变换，把A化为

$$A_1=\begin{pmatrix} d & a_{11} & a_{12}\cdots & a_{1s} \\ 0 & a_{21} & a_{22}\cdots & a_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a_{s1} & a_{s2}\cdots & a_{ss} \end{pmatrix},$$

从A_1可证

定理3 如果$d\nmid n$，则方程(1)没有整数解；如果$d\mid n$，则方程(1)的全部解为

$$x_1 = a_{11}\frac{n}{d} + a_{21}t_2 + a_{31}t_3 + \cdots + a_{s1}t_s,$$

$$x_2 = a_{12}\frac{n}{d} + a_{22}t_2 + a_{32}t_3 + \cdots + a_{s2}t_s,$$

$$\cdots\cdots\cdots$$

$$x_s = a_{1s}\frac{n}{d} + a_{2s}t_2 + a_{3s}t_3 + \cdots + a_{ss}t_s,$$

其中$t_i(i=2, \cdots, s)\in Z$。

应该指出，还可以用其他的一些方法给出方程(1) 的全部解。

这些工作的动力主要是基于整数线性规化和整系数线性型问题的研究。整系数线性型问题在合理下料等实际问题上有重要应用。

§3 整系数线性型问题

求$s\geqslant 2$元一次丢番图方程

$$a_1x_1 + \cdots + a_sx_s = n, (a_1, \cdots, a_s) = 1 \tag{1}$$

的非负整数解，只要在(1)的整数解中令$x_i\geqslant 0(i=1,\cdots,s)$解出所含参数的范围就行了。现在的问题是，任给一个正整数n，不需要解方程(1)，怎样知道(1)是否存在非负整数解？Frobenius 提出了一个所谓整系数线性型问题，即任给正整数$a_i(i=1,\cdots,s)$，$(a_1,\cdots,a_s)=1$，求一个仅与$a_i(i=1,\cdots,s)$有关的整数$g(a_1,\cdots,a_s)$，在$n>g(a_1,\cdots,a_s)$时，方程(1)有非负整数解$x_i(i=1,\cdots,s)$，而在$n=g(a_1,\cdots,a_s)$时方程(1)无非负整数解。这里的$g(a_1,\cdots,a_s)$称为整系数线性型的最大不可表数。下面我们来介绍$g(a_1,\cdots,a_s)$的求法。

定理1　在$s=2$时，$g(a_1,\ a_2)=a_1a_2-a_1-a_2$。

证　因为$(a_1,\ a_2)=1$，故由§1知，在$s=2$时，方程(1)的全部解可表为

$$x_1=x_1^{(0)}+a_2t,\quad x_2=x_2^{(0)}-a_1t,\quad t\in Z, \tag{2}$$

这里$x_1^{(0)}$，$x_2^{(0)}$为$s=2$时(1)的任一组解。

首先证明在$n>a_1a_2-a_1-a_2$时，(2)式可取t使$x_1\geqslant 0$，$x_2\geqslant 0$。因为$x_2=x_2^{(0)}-a_1t$可写成$x_2=a_1t'+\langle x_2^{(0)}\rangle_{a_1}$，故可取 t 使得

$$0\leqslant x_2=x_2^{(0)}-a_1t<a_1,$$

即

$$0\leqslant x_2^{(0)}-a_1t\leqslant a_1-1。$$

故由$n>a_1a_2-a_1-a_2$知

$$\begin{aligned}x_1a_1&=n-(x_2^{(0)}-a_1t)a_2\\&>a_1a_2-a_1-a_2-(a_1-1)a_2=-a_1。\end{aligned}$$

由此即得$x_1>-1$，从而$x_1\geqslant 0$。这就证明在$n>a_1a_2-a_1-a_2$时可取t使$x_1\geqslant 0$，$x_2\geqslant 0$。

再证$n=a_1a_2-a_1-a_2$时，方程(1)在$s=2$时无非负整数解。不然，可设有非负整数x_1，x_2适合

$$a_1x_1+a_2x_2=a_1a_2-a_1-a_2,$$

由此知

$$a_1a_2=a_1(x_1+1)+a_2(x_2+1)。 \tag{3}$$

因为$(a_2,\ a_2)=1$，故$a_1\mid x_2+1$，$a_2\mid x_1+1$，故$x_2+1\geqslant a_1$，$x_1+1\geqslant a_2$，所以(3)式给出

$$a_1a_2\geqslant a_1a_2+a_2a_1,$$

此由a_1，a_2是正整数知不可能。证毕。

在$s\geqslant 3$时，求 $g(a_1,\cdots,a_s)$是一个困难的问题。1955年柯召[3]首先讨论了$s=3$的情形，证明了

定理2 $g(a_1,a_2,a_3)\leqslant\frac{a_1a_2}{(a_1,\ a_2)}+a_3(a_1,\ a_2)-a_1-a_2-a_3$。且当 $n>\frac{a_1a_2}{(a_1,a_2)^2}-\frac{a_1}{(a_1,\ a_2)}-\frac{a_2}{(a_1,\ a_2)}$时有

$$g(a_1,a_2,a_3)=\frac{a_1a_2}{(a_1,\ a_2)}+a_3(a_1,\ a_2)-a_1-a_2-a_3,$$

这里a_1，a_2，a_3可以轮换。

1956年，陈重穆[4]把定理2推广到任意$s\geqslant3$上，即有

定理3 设 $d_i=(a_1,\cdots,a_i)$ $(i=2,\cdots,s)$，$d_1=a_1$及

$G_i=\sum\limits_{j=2}^{i}a_j\frac{d_{j-1}}{d_j}-\sum\limits_{j=1}^{i}a_j$ $(i=2,\ \cdots,\ s)$，则

$$g(a_1,\cdots,a_s)\leqslant G_s,$$

且当$a_j\frac{d_{j-1}}{d_j}>G_{j-1}$ $(3\leqslant j\leqslant s)$时，则$g(a_1,\cdots,a_s)=G_s$。

1957年，陆文端和吴昌玖[5]证明了$g(a_1,\cdots,a_s)=G_s$的充要条件是$a_j\frac{d_{j-1}}{d_j}$可经线性型f_{j-1}表出$(j=3,\cdots,s)$，这里f_{j-1}定义为下面的线性型

$$f_s=a_1x_1+\cdots+a_sx_s,\quad x_i\geqslant0\ (i=1,\cdots,s),$$

其中$a_1,\cdots,a_s$为正整数，$(a_1,\cdots,a_s)=1$。令

$$\lambda_i=(a_1,\cdots,a_{i-1},\ a_{i+1},\ \cdots\ ,a_s)\quad(i=1,\cdots,s),$$

因为$(a_1,\cdots,a_s)=1$，故

$$(a_i,\ \lambda_i)=1\ \ (i=1,\cdots,s),$$
$$(\lambda_i,\ \lambda_j)=1\ \ (1\leqslant i\neq j\leqslant s)。$$

再令

$$a_i=b_i\lambda_1\cdots\lambda_{i-1}\lambda_{i+1}\cdots\lambda_s\quad(i=1,\cdots,s),$$
$$D_i=(b_1,\cdots,b_i)\quad(i=1,\cdots,s),$$

则$D_s=D_{s-1}=1$及

$$d_i=(a_1,\cdots,a_i)=\lambda_{i+1}\cdots\lambda_s D_i\ (i=1,\cdots,s)。$$

记

$$\overline{G}_i=\sum_{j=2}^{i}b_j\frac{D_{j-1}}{D_j}-\sum_{j=1}^{i}b_j\ (i=2,\cdots,s),$$

显然有$\overline{G}_{s-1}=\overline{G}_s$。陆文端与吴昌玖证明了

定理4 $g(a_1,\cdots,a_s)=g(b_1,\cdots,b_s)\lambda_1\cdots\lambda_s+\sum_{i=1}^{s}a_i(\lambda_i-1)$。

定理5 一般的$g(a_1,\cdots,a_s)$有形式

$$g(a_1,\cdots,a_s)=G_s-\sum_{i=1}^{s}a_i\lambda_i t_i,\ t_i\geqslant 0\ (i=1,\cdots,s)。$$

定理6 线性型f_s不能表出的整数L都可以写成如下的形式

$$L=\sum_{i=2}^{s}a_i\frac{d_{i-1}}{d_i}-\sum_{i=1}^{s}a_it_i=G_s-\sum_{i=1}^{s}a_i(t_i-1),$$

这里$t_i\geqslant 1$ $(i=1,\cdots,s)$。

后来，李培基[6]、尹文霖[7]还给出了进一步的讨论，例如尹文霖证明了

定理 7 设$d_{s-1}=(a_1,\cdots,a_{s-1})$，$M^*_{s-1}=\left\{m:m=\sum_{i=1}^{s-1}\frac{a_i}{d_{s-1}}x_i\text{且}x_i\geqslant 0\ (i=1,\cdots,s)\right\}$，$K$适合$Ka_s\in M^*_{s-1}$的最小正整数，则

$$g(a_1,\cdots,a_s)=\max_{\substack{\overline{n}-ka_s\in M^*_{s-1}\\ 0\leqslant k<K}}(d_{s-1}\overline{n}+a_s(d_{s-1}-1))。$$

推论　$g(a_1,a_2,a_3)=\dfrac{a_1a_2}{(a_1,\ a_2)}-a_1-a_2-a_3$

$$-(n^*-a_3)(a_1,\ a_2),$$

其中$n^*=\min\limits_{\substack{m+ka_3\in M_2^*\\ 0\le k<K}} m$。

由定理7可以推出定理 4、5和6。为了证明定理7，除了使用前面的符号，我们引进以下的符号：

$$M_j=\left\{m:m=\sum_{i=1}^{j}a_ix_i,\ \ x_i\geqslant 0\ \ (i=1,\cdots,j)\right\},$$

$$\overline{M}_j=\left\{m:m\overline{\in}M_j,\ m\text{是整数}\right\},$$

$$M_j^*=\{m:md_j\in M_j\},$$

$$\overline{M}_j^*=\left\{m:md_j\overline{\in}M_j,\ m\text{是整数}\right\},$$

$$\overline{M}_j(r)=\left\{m:m\equiv\frac{a_j}{d_j}r(\mathrm{mod}\,d_{j-1}^*),m\in\overline{M}_j\right\},$$

式中

$$d_{j-1}^*=\frac{d_{j-1}}{d_j},\ \ 0\leqslant r<d_{j-1}^*\ \ (j=2,\cdots,s)。$$

由于$(d_{s-1},\ a_s)=1$，故

$$\overline{M}_s=\bigcup_{0\le r<d_{s-1}}\overline{M}_s(r)。\tag{4}$$

显然还有

$$\overline{M}_s(r)\subseteq d_{s-1}\overline{M}_{s-1}^*+a_sr,\tag{5}$$

式中数与集合相乘和相加，定义为：设A是集合，a 是数，则$aA=\{m:m=an,n\in A\}$，$A+a=\{m:m=n+a,n\in A\}$。令K表示满足条件

$$Ka_s\in M_{s-1}^*$$

的最小正整数。设$m>0$，则存在唯一的r，$0\leqslant r<d_{s-1}$，使$m\equiv a_s r(\bmod d_{s-1})$成立，令

$$m(r,k)=m-a_s r-ka_s d_{s-1},\quad 0\leqslant k<K。$$

又设

$$P_j=\{p:p\in\overline{M}_j,p+a_i\in M,\ (i=1,\ \cdots,j)\},$$
$$P_j^*=\{p:pd_j\in P_j\}。$$

显然有

$$\overline{M}_s=P_s-n,\quad n\in M_s。\tag{6}$$

这里集合A与数a的减法定义为：$A-a=\{m:m=n-a,n\in A\}$。

引理 1 $m\in\overline{M}_s$的充要条件是$m(r,k)\in\overline{M}_{s-1}$，$0\leqslant k<K$，$0\leqslant r<d_{s-1}$。

证 设$m\in\overline{M}_s$，由$m=m(r,k)+a_s(r+kd_{s-1})$
$\equiv a_s r(\bmod d_{s-1})$知，若存在$r$，$k$使$m(r,k)\in M_{s-1}$，则$m\in M_s$，与$m\in\overline{M}_s$矛盾，故必要性得证。

现证充分性。设$m(r,k)\in\overline{M}_{s-1}$，$0\leqslant k<K$，$0\leqslant r<d_{s-1}$，如果$m\in M_s$，则

$$m=a_1x_1+\cdots+a_{s-1}x_{s-1}+a_n(R+tKd),$$

式中$0\leqslant R<Kd$，$t\geqslant 0$，$x_i\geqslant 0$ $(i=1,\cdots,s-1)$。按K的定义，存在某$r,k(0\leqslant r<d_{s-1}$，$0\leqslant k<K)$使得

$$m=a_1y_1+\cdots+a_{s-1}y_{s-1}+a_s(r+kd),$$

此即$m(r,k)\in M_{s-1}$，与假设矛盾。证华。

引理 2 P_s中的数p必具有形式

$$p=d_{s-1}\overline{n}+a_s(d_{s-1}-1),\tag{7}$$

其中$\overline{n}$满足条件

$$\overline{n}-ka_s\in\overline{M}^*_{s-1},\ 0\leqslant k<K。\tag{8}$$

并且$\overline{M}_s$中满足条件(8)且具有(7)的形式的最大数$p^*\in P_s$。

证 设$p\in P_s$，由于$P_s\subseteq\overline{M}_s$，故$p\in\overline{M}_s$。由引理1知

$$p=d_{s-1}\overline{n}+a_s r,$$

这里r为满足$p\equiv a_s r(\bmod d_{s-1})$的最小非负整数，且

$$\overline{n}-ka_s=\frac{1}{d_{s-1}}p(r,k)\in\overline{M}^*_{s-1},\ 0\leqslant k<K,$$

故只要证$r=d-1$即可。不然，令$m=p+a_s$，则

$$m(r+1,\ k)=p(r,\ k)\in d_{s-1}\overline{M}^*_{s-1}。$$

而由定义知$\overline{M}_{s-1}=d_{s-1}\overline{M}^*_{s-1}$，故$m(r+1,\ k)\in\overline{M}_{s-1}$，由引理1知$m\in\overline{M}_s$，这与$m=p+a_s\in P_s$矛盾。这就证明了引理的前半部论断。

现设$p^*\overline{\in}P_s$，则由(6)式知

$$p^*=p-m,\ 0<m\in M_s,\ p\in P_s,$$

由引理的前半部论断知，p适合(8)且具有形式(7)，这就与最大性矛盾。证毕。

定理7的证明： 由前面讨论，及引理知

$$g(a_1,\cdots,a_s)=\max_{m\in\overline{M}_s} m=\max_{p\in P_s} p$$

$$=\max_{\substack{\overline{n}-ka_s\in\overline{M}^*_{s-1}\\0\leqslant k<K}}(d_{s-1}\overline{n}+a_s(d_{s-1}-1))$$

$$=\max_{\substack{\overline{n}-ka_s\in M^*_{s-1}\\0\leqslant k<K}}(d_{s-1}\overline{n}+a_s(d_{s-1}-1))。$$证毕。

至于推论的证明，只要注意到条件(8) 在代换$\overline{n}=p_{s-1}-m$下，对m而言有等价条件

$$p'_{s-1}-p_{s-1}+m+ka_s\in M^*_{s-1},\quad 0\leqslant k<K,$$

这里p_{s-1}，p'_{s-1}独立地取遍P^*_{s-1}中各元素。

例 求$g(21,22,30)$。

解 取$a_1=30$，$a_2=21$，$a_3=22$,则$(a_1,a_2)=3$。又K是满足

$$22K\in M^*_2=\{m:3m\in M_2\}$$

的最小正整数，而

$$3\cdot 22=30x_1+21x_2,\quad x_1\geqslant 0,\quad x_2\geqslant 0$$

无解，故$22\overline{\in}M^*_2$。这样由

$$3\cdot(2\cdot 22)=3\cdot 30+2\cdot 21$$

知$K=2$。于是$n^*=\min\limits_{\substack{m+22k\in M^*_2\\ k=0,1}} m=20$，所以

$$g(21,22,30)=\frac{30\cdot 21}{3}-30-21-22-(20-22)\cdot 3$$

$$=210-73+6=143。$$

关于线性型，还有另外的一些研究。例如，1956年Roberts[8]曾讨论了$a_1,\cdots,a_s$成等差数列的情形，证明了

定理 8 设$a_j=a_1+jd(j=2,\cdots,s)$,这里$a_1\geqslant 2,d>0$,则

$$g(a_1,\cdots,a_s)=\left[\frac{a_1-2}{s-1}\right]a_1+(a_1-1)d。$$

1958年,吴昌玖[9]给出了定理8的一个十分简短的证明,并且顺便得出了线性型不能表出的正整数的个数。

1984年，万大庆和王西京[10]发现，以往所有关于$g(a_1,\cdots,a_s)$的工作说明，在$s\geqslant 3$时，$g(a_1,\cdots,a_s)$都不是

关于$a_1,\cdots,a_s$的多项式($s=2$时$g(a_1, a_2)=a_1a_2-a_1-a_2$是关于$a_1,\cdots,a_s$的多项式)。一般的情况如何呢？万大庆和王西京证明了

定理 9 在$s\geqslant 3$时，不存在多项式$h(x_1,\cdots,x_s)$，使得当正整数$a_i(i=1,\cdots,s)$两两互素时，$g(a_1,\cdots,a_s)=h(a_1,\cdots,a_s)$。

证 在正整数$a_i(i=1,\cdots,s)$两两互素时，若存在多项式h，则$h\neq 0$。记$h(x_1,\cdots,x_s)$关于x_s的次数是n_s，$x_s^{n_s}$的系数是$h_{s-1}(x_1,\cdots,x_{s-1})$（显然$h_{s-1}\neq 0$）；$h_{s-1}(x_1,\cdots,x_{s-1})$关于$x_{s-1}$的次数是$n_{s-1}$，$x_{s-1}^{n_{s-1}}$的系数是$h_{s-2}(x_1,\cdots,x_{s-2})$；…。如此可得到均不恒为0的一列多项式：$h_1(x)$，$h_2(x_1, x_2)$，…，$h_{s-1}(x_1,\cdots,x_{s-1})$。其中$h_i(x_1,\cdots,x_i)$是$h_{i+1}(x_1,\cdots,x_{i+1})$中$x_{i+1}$的最高次项的系数。

现取定$a_1>0$，使$h_1(a_1)\neq 0$；再取定$a_2>0$，$(a_1,a_2)=1$，使$h_2(a_1, a_2)\neq 0$；…。这样可得到一列两两互素的正整数$a_1,\cdots,a_s$，使得$h_{s-1}(a_1,\cdots,a_{s-1})\neq 0$。

这样，只要$(x_s, a_1\cdots a_{s-1})=1$，$x_s>0$，就有$g(a_1,\cdots,a_{s-1}, x_s)=h(a_1,\cdots,a_{s-1}, x_s)$。从$s\geqslant 3$得到

$$0\leqslant g(a_1,\cdots,a_{s-1}, x_s)\leqslant g(a_1, a_2)。$$

由此知$h(a_1,\cdots,a_{s-1}, x_s)$有界($x_s\to\infty$)，推出$h(x_1,\cdots,x_s)$与$x_s$无关。同理，$h(x_1,\cdots,x_s)$与任一变元都无关，即$h(x_1, \cdots, x_s)$为常数。这是不可能的。证毕。

用类似的方法，还可证明：在$s\geqslant 3$时，不存在有理分式$E(x_1,\cdots,x_s)$，使$g(a_1,\cdots,a_s)=E(a_1,\cdots, a_s)$。

最后，借用前面的符号和归纳法可得：若$n\overline{\in} M_s$，则$G_s-n\in M_s$。

参 考 文 献

[1] 徐肇玉、曹珍富，哈尔滨工业大学学报，数学增刊(1984)，142—150。

[2] 凌露娜，华南师范大学学报(自然科学版)，1(1985)，66—71。

[3] 柯召，四川大学学报（自然科学版），1(1955)，1—4。

[4] 陈重穆，四川大学学报（自然科学版），1956，No.1。

[5] 陆文端、吴昌玖，四川大学学报（自然科学版），2(1957)，151—171。

[6] 李培基，四川大学学报（自然科学版），3(1959)，43—50。

[7] 尹文霖，高等学校自然科学学报（数学、力学、天文学版），试刊，1(1964)，32—38。

[8] Roberts, J.B., Proc. Amer. Math. Soc., 7(1956), 465—469。

[9] 吴昌玖，四川大学学报（自然科学版），1(1958)，33—36。

[10] 万大庆，王西京，数学汇刊，1(1984)，76—78。

第五章　二次丢番图方程

本章讨论二次丢番图方程的解法。

§1　一般的二元二次丢番图方程

一般的二元二次丢番图方程是指二次型方程

$$ax^2+bxy+cy^2+dx+ey+f=0。\tag{1}$$

令$D=b^2-4ac$，若$D=0$，则以$4a$乘(1)式得

$$(2ax+by)^2+4adx+4aey+4af=0。$$

令　$2ax+by=t$，上式化为

$$t^2+2dt+2(2ae-bd)y+4af=0,$$

于是

$$(t+d)^2=2(bd-2ae)y+d^2-4af。$$

此方程的求解等价于同余式$(t+d)^2\equiv d^2-4af(\bmod 2(bd-2ae))$的求解，因此此时方程(1)的求解较易。

现设$D\neq 0$，以D^2乘(1)式得

$$aD^2x^2+bD^2xy+cD^2y^2+dD^2x+eD^2y+fD^2=0,$$

令　$Dx=x'+2cd-be$，$Dy=y'+2ae-bd$代入上式得

$$a(x'+2cd-be)^2+b(x'+2cd-be)(y'+2ae-bd)+c(y'+2ae-bd)^2+dD(x'+2cd-be)+eD(y'+2ae-bd)+fD^2=0,$$

即

$$ax'^2+bx'y'+cy'^2=D\Delta,\tag{2}$$

这里$\Delta=4acf+bde-ae^2-cd^2-fb^2$ 称为二次型(1)的判别式。显然，如果$a=0$，(2)式化为$y'(bx'+cy')=D\Delta$，故十分容易求解。因此可设$a\neq 0$，以$4a$乘(2)式两端化为

$$(2ax'+by')^2-Dy'^2=4aD\Delta,$$

令 $X=2ax'+by'$，$Y=y'$，$M=4aD\Delta$，则上式化为

$$X^2-DY^2=M。\qquad (3)$$

由此可见，求一般的二元二次丢番图方程，主要依赖于方程(3)的解决。又，如果D是平方数或$D\leqslant 0$，则对给定的M，方程(3)也容易解决，故以下设 $D>0$ 且不是平方数。

如果方程(3)有解，显然$M\neq 0$。由第三章§1 知，在二次域$Q(\sqrt{D})$ 中，方程(3)可化为

$$X+Y\sqrt{D}=\pm\varepsilon^n\eta,\ \eta\in K,\ n\in Z,\qquad (4)$$

这里ε是$Q(\sqrt{D})$的基本单位数，$N(\varepsilon)=1$，$N(\eta)=M$，且K是 $Z[\sqrt{D}]$的一个有限子集。显然对 $\forall\eta\in K$，(4)式均给出方程(3)的无穷多组解。后面，我们将用初等方法给出ε和K的结构和求法。

§2 Pell方程$x^2-Dy^2=1$

现在我们来解决上节(3)式的一些特例，即给出Pell方程$x^2-Dy^2=1$的全部整数解（参阅第二章§6）。

我们在第三章§4中曾经介绍过Dirichlet关于丢番图逼近的一个结果，即

引理 设θ是一个无理数，则有无穷多对整数x，$y>0$适合不等式

$$\left|\frac{x}{y}-\theta\right|<\frac{1}{y^2}。\qquad (1)$$

证 设任给正整数$n>1$,由θ为无理数知,当y取$0,1,\cdots,n$时,取$x=[y\theta]+1$([·]表·的整数部分),则有

$$0\leqslant x-y\theta<1。\tag{2}$$

于是知,有$n+1$对x,y适合(2)式。现把$[0,1)$分成n个区间$[\frac{r}{n},\frac{r+1}{n})$ $(r=0,1,\cdots,n)$,则由抽屉原理知,必有整数对x_1,y_1和x_2,y_2使得$x_1-y_1\theta$和$x_2-y_2\theta$同属某一个区间$\left[\frac{j}{n},\frac{j+1}{n}\right)$ $(0\leqslant j<n)$,于是

$$|(x_1-y_1\theta)-(x_2-y_2\theta)|<\frac{1}{n},\tag{3}$$

这里不失一般可设$y_1>y_2$。令$x^{(1)}=x_1-x_2$,$y^{(1)}=y_1-y_2$,由y_1,$y_2\in\{0,1,\cdots,n\}$及$y_1>y_2$知$0<y^{(1)}\leqslant n$,故由(3)得

$$|x^{(1)}-y^{(1)}\theta|<\frac{1}{n}\leqslant\frac{1}{y^{(1)}}。$$

由于$|x^{(1)}-y^{(1)}\theta|>0$,故可取整数$n_1>1$使得

$$\frac{1}{n_1}<|x^{(1)}-y^{(1)}\theta|<\frac{1}{y^{(1)}},$$

对n_1重复前面的作法可知,存在整数$x^{(2)}$,$y^{(2)}>0$使

$$|x^{(2)}-y^{(2)}\theta|<\frac{1}{n_1}\leqslant\frac{1}{y^{(2)}}。$$

以上步骤可以一直作下去,得到

$$|x^{(1)}-y^{(1)}\theta|>\frac{1}{n_1}>|x^{(2)}-y^{(2)}\theta|>\cdots$$

即有无穷多组不同的整数对$x^{(i)}$,$y^{(i)}>0$ $(i=1,2,\cdots)$适合

$$|x-y\theta|<\frac{1}{y}\quad 或\quad \left|\frac{x}{y}-\theta\right|<\frac{1}{y^2},$$

这就证明了引理。证毕。

定理 1 设$D>0$且不是平方数，则存在整数M，$0<|M|<1+2\sqrt{D}$，使得方程

$$x^2-Dy^2=M \tag{4}$$

有无穷多组整数解x，$y>0$。

证 在(1)中取$\theta=\sqrt{D}$，则由引理知，存在无穷多组整数x，$y>0$使

$$\left|\frac{x}{y}-\sqrt{D}\right|<\frac{1}{y^2}\text{，即}\ |x-y\sqrt{D}|<\frac{1}{y}。$$

而

$$|x+y\sqrt{D}|=|x-y\sqrt{D}+2y\sqrt{D}|<\frac{1}{y}+2y\sqrt{D}，$$

故存在无穷多组整数x，$y>0$使

$$|x^2-Dy^2|<\frac{1}{y}\left(\frac{1}{y}+2y\sqrt{D}\right)=\frac{1}{y^2}+2\sqrt{D}\leqslant 1+2\sqrt{D}。$$

因为$|M|<1+2\sqrt{D}$的整数M仅有有限个，故对某M，$|M|<1+2\sqrt{D}$，方程(4)有无穷多组解。由于(4)给出$M\neq 0$，故$|M|>0$。证毕。

定理 2 设$D>0$且不是平方数，则Pell方程

$$x^2-Dy^2=1 \tag{5}$$

至少有一组正整数解。

证 由定理1知，(4)有无穷多组正整数解x，y。因此(4)至少有两组不同的正整数解(x_1,y_1)和(x_2,y_2)满足

$$x_1\equiv x_2(\bmod |M|),\quad y_1\equiv y_2(\bmod |M|),$$

由此推出

$$x_1x_2-Dy_1y_2\equiv x_1^2-Dy_1^2=M\equiv 0\ (\bmod |M|),$$

$$x_1y_2-x_2y_1\equiv x_2y_2-x_2y_2=0(\bmod |M|)。$$

而由

$$M^2=(x_1^2-Dy_1^2)(x_2^2-Dy_2^2)=(x_1x_2-Dy_1y_2)^2$$
$$-D(x_1y_2-x_2y_1)^2$$

知

$$\left(\frac{x_1x_2-Dy_1y_2}{M}\right)^2-D\left(\frac{x_1y_2-x_2y_1}{M}\right)^2=1,$$

这就给出方程(5)有非负整数解 $x=\left|\frac{x_1x_2-Dy_1y_2}{M}\right|$,

$y=\left|\frac{x_1y_2-x_2y_1}{M}\right|$。下面只要证明$\left|\frac{x_1y_2-x_2y_1}{M}\right|\neq 0$,

因为不然有 $x_1y_2=x_2y_1$,故可设$\frac{x_1}{x_2}=\frac{y_1}{y_2}=t>0$,由$x_1=tx_2$, $y_1=ty_2$代入(4)得

$$M=t^2x_2^2-Dt^2y_2^2=t^2M,$$

此推出$t=1$,即$x_1=x_2$, $y_1=y_2$,与(x_1, y_1)和(x_2,y_2)是(4)的不同解矛盾。这就证明了定理2。证毕。

从定理2,可设x_0, y_0是Pell 方程(5)的所有正整数解x, y中使 $x+y\sqrt{D}$为最小的解。称(x_0, y_0)为 Pell 方程(5)的最小解,或称$x_0+y_0\sqrt{D}$为Pell 方程(5)的基本解。

定理 3 设$x_0+y_0\sqrt{D}$是Pell 方程(5)的基本解,则(5)的全部整数解可表为

$$x+y\sqrt{D}=\pm(x_0+y_0\sqrt{D})^n,\ n\in Z。\qquad (6)$$

证 记$\varepsilon=x_0+y_0\sqrt{D}$。$\bar{\varepsilon}=x_0-y_0\sqrt{D}$, $\varepsilon\bar{\varepsilon}=1$。首先证明(6)给出的$x,y$确为方程(5)的解。因为由$x+y\sqrt{D}=\pm\varepsilon^n$知 $x-y\sqrt{D}=\pm\bar{\varepsilon}^n$,故$x^2-Dy^2=(\varepsilon\bar{\varepsilon})^n=1$。

下面我们来证明方程(5)的任一组整数解均可表为(6)。由于$\varepsilon^{-1}=\bar{\varepsilon}$，故只需证明(5)的任一组正整数解可表为

$$x+y\sqrt{D}=\varepsilon^{n},\quad n>0 \tag{7}$$

即可。为此，可设(5)有正整数解x，y不能表为(7)的形状，于是由$x+y\sqrt{D}>\varepsilon$知，必有正整数n使得

$$\varepsilon^{n}<x+y\sqrt{D}<\varepsilon^{n+1},$$

两端乘以$\bar{\varepsilon}^{n}$，则得出

$$1<(x+y\sqrt{D})\bar{\varepsilon}^{n}<\varepsilon。\tag{8}$$

可令$u+v\sqrt{D}=(x+y\sqrt{D})\bar{\varepsilon}^{n}$，则$u^{2}-Dv^{2}=1$，即$u,v$为方程(5)的一组解。由(8)知$u+v\sqrt{D}>1$，故$0<u-v\sqrt{D}=\dfrac{1}{u+v\sqrt{D}}<1$,所以$u>0$。又$2v\sqrt{D}=(u+v\sqrt{D})-(u-v\sqrt{D})>1-1=0$，故$v>0$。这就证明$u$，$v$为(5)的一组正整数解，因此$u+v\sqrt{D}>\varepsilon$，这与(8)矛盾。证毕。

这个定理告诉我们，求方程(5)的全部整数解可归结为找它的一组最小解。求Pell 方程(5)的最小解，是一件十分麻烦的事情。一般说来，令$y=1,2,3,\cdots$,代入$1+Dy^{2}$使它出现第一个平方数的那组值即为(5)的最小解。但用这种方法，有时的计算十分冗长，例如 Pell方程$x^{2}-1141y^{2}=1$当$1\leqslant y\leqslant 10^{25}$时都无解，它的基本解$x_{0}+y_{0}\sqrt{1141}$中的$y_{0}=30693385322765657197397208$。

在一些问题的研究中，常常要确定Pell 方程(5)的一组解是否是基本解。我们有

定理 4 设x_{1}，y_{1}是方程(5)的一组正整数解。如果

$$x_{1}>\frac{1}{2}y_{1}^{2}-1,\tag{9}$$

则 $x_1+y_1\sqrt{D}$是方程(5)的基本解。

证 如果$y_1=1$，则$x_1+y_1\sqrt{D}$显然是(5)的基本解。现设$y_1>1$，如果$x_1+y_1\sqrt{D}$不是(5)的基本解，则可令$\varepsilon=x_0+y_0\sqrt{D}$是(5)的基本解，$1\leqslant y_0<y_1$，于是

$$x_0^2y_1^2-y_0^2x_1^2=y_1^2(1+Dy_0^2)-y_0^2x_1^2$$
$$=y_1^2-y_0^2(x_1^2-Dy_1^2)=y_1^2-y_0^2>0,$$

由此得

$$x_0y_1+y_0x_1=\xi,\ x_0y_1-y_0x_1=\eta,\ y_1^2-y_0^2=\xi\eta,$$

其中$\xi>0$，$\eta>0$。这样就有

$$x_1=\frac{\xi-\eta}{2y_0}\leqslant\frac{y_1^2-y_0^2-1}{2y_0}\leqslant\frac{1}{2}y_1^2-1,$$

与(9)式矛盾。证毕。

推论 设$s>0,t>0,D=s(st^2+2)$，则方程$x^2-Dy^2=1$的基本解$x_0+y_0\sqrt{D}=1+st^2+t\sqrt{D}$。

证 由于$x_1=1+st^2$，$y_1=t$是方程$x^2-Dy^2=1$的正整数解，且满足$x_1>\frac{1}{2}y_1^2-1$，故由定理4知推论为真。证毕。

§3 方程$x^2-Dy^2=M$

设$D>0$且不是平方数，$M\neq0$都是给定的整数，我们来解丢番图方程

$$x^2-Dy^2=M。\tag{1}$$

以下都设方程(1)有解。如果x_1，y_1为方程(1)的一组解，则为了方便，我们也称$x_1+y_1\sqrt{D}$为方程(1)的一个解。

再设$s+t\sqrt{D}$是Pell方程

$$x^2-Dy^2=1 \tag{2}$$

的任一解，则有

$$(x_1+y_1\sqrt{D})(s+t\sqrt{D})=x_1s+y_1tD+(y_1s+x_1t)\sqrt{D},$$

且容易验证

$$(x_1s+y_1tD)^2-D(y_1s+x_1t)^2=M。$$

这就得出$(x_1+y_1\sqrt{D})(s+t\sqrt{D})$也是(1)的解。我们称这个解与$x_1+y_1\sqrt{D}$相结合。设(1)的两个解$x_1+y_1\sqrt{D}$和$x_2+y_2\sqrt{D}$相结合（记为$x_1+y_1\sqrt{D}\sim x_2+y_2\sqrt{D}$），显然有

1） $x_1+y_1\sqrt{D}\sim x_1+y_1\sqrt{D}$；

2） 如果 $x_1+y_1\sqrt{D}\sim x_2+y_2\sqrt{D}$，则

$$x_2+y_2\sqrt{D}\sim x_1+y_1\sqrt{D};$$

3） 设$x_3+y_3\sqrt{D}$也是(1)的解，且有$x_1+y_1\sqrt{D}\sim x_2+y_2\sqrt{D}$，$x_2+y_2\sqrt{D}\sim x_3+y_3\sqrt{D}$，则
$x_1+y_1\sqrt{D}\sim x_3+y_3\sqrt{D}$。

由1)～3)知，相结合～是等价关系（与同余关系类似），故如果(1)有解，可将(1)的全部解用相结合关系进行分类，每一类中的解彼此相结合，且不在同一类中的任两解均不相结合。

定理 1 方程(1)的两个解$x_1+y_1\sqrt{D}$和$x_2+y_2\sqrt{D}$同属某类K的充要条件是

$$x_1x_2-Dy_1y_2\equiv 0(\bmod |M|),\quad y_1x_2-x_1y_2\equiv 0(\bmod |M|)。\tag{3}$$

证 设$x_1+y_1\sqrt{D}\sim x_2+y_2\sqrt{D}$,则(2)存在解$s+t\sqrt{D}$使得

$$x_1+y_1\sqrt{D}=(x_2+y_2\sqrt{D})(s+t\sqrt{D})$$
$$=x_2s+Dy_2t+(x_2t+y_2s)\sqrt{D},$$

故$x_1=x_2s+Dy_2t$，$y_1=x_2t+y_2s$。由此解出

$$s=\frac{x_1x_2-Dy_1y_2}{x_2^2-Dy_2^2}=\frac{x_1x_2-Dy_1y_2}{M},$$

$$t=\frac{y_1x_2-x_1y_2}{x_2^2-Dy_2^2}=\frac{y_1x_2-x_1y_2}{M},$$

故(3)成立。

由于上面推导步步可逆，故定理1得到证明。证毕。

由定理1知，设$x_1+y_1\sqrt{D}$是方程(1)的任一解，则$-(x_1+y_1\sqrt{D})\sim x_1+y_1\sqrt{D}$，$-(x_1-y_1\sqrt{D})\sim x_1-y_1\sqrt{D}$。设$K$和$\overline{K}$是(1)的解的任意两个结合类，如果任给$x+y\sqrt{D}\in K$，都有$x-y\sqrt{D}\in\overline{K}$，且反之亦然，则称$K$和$\overline{K}$互为共轭类。如果$K=\overline{K}$，则$K$称为歧类。

设$u_0+v_0\sqrt{D}$是某结合类K的基本解,它是按如下方式选择的：首先,当K不是歧类时,$u_0+v_0\sqrt{D}$是K中所有$v\geqslant0$的解$u+v\sqrt{D}$中使v最小的那组解。由于$-u_0+v_0\sqrt{D}=-(u_0-v_0\sqrt{D})\in\overline{K}$，故$u_0$是唯一的；其次，当$K$是歧类时，$v_0$的选择如前，而$u_0$选择含$v_0$的解$u+v_0\sqrt{D}$中使得$u\geqslant0$的那个。

定理 2 设K是方程(1)解的任一结合类，$u_0+v_0\sqrt{D}$是K的基本解。再设$x_0+y_0\sqrt{D}$是方程(2)的基本解，则有

$$0\leqslant v_0\leqslant\begin{cases}\dfrac{y_0\sqrt{M}}{\sqrt{2(x_0+1)}}, & 当M>0;\\ \dfrac{y_0\sqrt{-M}}{\sqrt{2(x_0-1)}}, & 当M<0。\end{cases}\tag{4}$$

$$0\leqslant|u_0|\leqslant\begin{cases}\sqrt{\dfrac{1}{2}(x_0+1)M}, & 当M>0;\\ \sqrt{\dfrac{1}{2}(x_0-1)(-M)}, & 当M<0。\end{cases}\tag{5}$$

证 这里只证$M>0$的情形($M<0$类似可证)。由于(4)和(5)对K成立，可推出对$\overline{K}$也成立，故不失一般性可设$u_0>0$。由于

$$(u_0+v_0\sqrt{D})(x_0-y_0\sqrt{D})\in K,$$

$$(u_0+v_0\sqrt{D})(x_0-y_0\sqrt{D})=u_0x_0-Dv_0y_0+(x_0v_0-y_0u_0)\sqrt{D},$$

且有

$$u_0x_0-Dv_0y_0=u_0x_0-\sqrt{(u_0^2-M)(x_0^2-1)}>0,$$

故由K的基本解$u_0+v_0\sqrt{D}$的定义易知

$$u_0x_0-Dv_0y_0\geqslant u_0,$$

由此知

$$u_0(x_0-1)\geqslant Dv_0y_0,\tag{6}$$

两边平方得

$$u_0^2(x_0-1)^2\geqslant D^2v_0^2y_0^2=(u_0^2-M)(x_0^2-1),$$

由此解出u_0^2得

$$u_0^2\leqslant\frac{1}{2}(x_0+1)M,即u_0\leqslant\sqrt{\frac{1}{2}(x_0+1)M}。$$

另外从(6)直接解出v_0得

$$v_0 \leqslant \frac{u_0(x_0-1)}{Dy_0} = \frac{u_0(x_0-1)y_0}{Dy_0^2}$$

$$= \frac{u_0 y_0}{x_0+1} \leqslant \frac{y_0\sqrt{\frac{1}{2}(x_0+1)M}}{x_0+1}$$

$$= \frac{y_0\sqrt{M}}{\sqrt{2(x_0+1)}}。$$ 证毕。

由定理 2 知方程(1)仅有有限个结合类，而且由(4)和(5)知，所有类的基本解可经有限步求出。显然，如果满足(4)和(5)的u_0，v_0均不是方程(1)的解，则方程(1)无解。

定理 3 设K是方程(1)解的一个结合类，$u_0+v_0\sqrt{D}$是K的基本解，则方程(1)的属于K类的全部解可由

$$x+y\sqrt{D}=\pm(u_0+v_0\sqrt{D})(x_0+y_0\sqrt{D})^n, n\in Z$$

表出，其中$x_0+y_0\sqrt{D}$是Pell方程(2)的基本解。

证 显然，上式给出的x，y是方程(1)属于K类的解。现设(1)的任一解$x+y\sqrt{D}\in K$，由定理1知

$$xu_0-Dyv_0\equiv 0(\bmod |M|), yu_0-xv_0\equiv 0(\bmod |M|),$$

令$X=\frac{xu_0-Dyv_0}{M}$，$Y=\frac{yu_0-xv_0}{M}$，则有$X^2-DY=1$

且$x+y\sqrt{D}=(u_0+v_0\sqrt{D})(X+Y\sqrt{D})$。故由Pell方程(2)的结果知

$$x+y\sqrt{D}=\pm(u_0+v_0\sqrt{D})(x_0+y_0\sqrt{D})^n, n\in Z。$$

证毕。

对于方程(1)，最后考虑几个特殊情形：$M=-1, \pm 2$和± 4。

Ⅰ．当$M=-1$时，方程(1)（也称为Pell方程）化为

$$x^2-Dy^2=-1。\tag{7}$$

如果(7)有整数解，则由定理1知，方程(7)仅有一个结合类。设$u_0+v_0\sqrt{D}$是基本解，由(7)知$v_0\neq 0$，$u_0\neq 0$，故可设$u_0>0$，$v_0>0$。此时$u_0+v_0\sqrt{D}$也称为(7)的基本解。

定理 4 如果Pell方程(7)有整数解，设$\delta=u_0+v_0\sqrt{D}$是基本解，则(7)的全部整数解可表为

$$x+y\sqrt{D}=\pm\delta^{2n-1}, n\in Z。$$

证 由定理3知，只要证明δ^2为Pell方程(2)的基本解$x_0+y_0\sqrt{D}$。首先容易验证δ^2确为方程(2)的解，故$\delta^2\geqslant x_0+y_0\sqrt{D}$。其次，由定理2知

$$\delta^2=(u_0+v_0\sqrt{D})^2\leqslant\left(\frac{y_0\sqrt{D}}{\sqrt{2(x_0-1)}}+\sqrt{\frac{x_0-1}{2}}\right)^2$$

$$=x_0+y_0\sqrt{D},$$

因此$\delta^2=x_0+y_0\sqrt{D}$。证毕。

设p是奇素数，从Pell方程(2)出发，可证方程$x^2-py^2=-1$(当$p\equiv 1 \pmod 4$)以及方程$x^2-2py^2=-1$(当$p\equiv 5 \pmod 8$)均有整数解。

但当D含有$4k+3$形因子或$D\equiv 0 \pmod 4$时，方程(7)均没有整数解。因此研究D取何值时，方程(7)有解或无解，是一件有意义的事情。1978年，Lienen[1]证明了

定理 5 设$p\equiv 1 \pmod 8$是素数且$2p=r^2+s^2$，$r\equiv\pm 3 \pmod 8$，$s\equiv\pm 3 \pmod 8$，则Pell方程(7)无解。

证 设此时方程(7)有解，由$p\equiv 1 \pmod 8$知，p可唯一地表为$p=a^2+b^2$，$0<a<b$，而$2p$可唯一表为$2p=r^2+s^2$，$0<r<s$。现在$2p=2(a^2+b^2)=(b-a)^2+(b+a)^2$，故

$$r=b-a,\quad s=b+a。$$

在$Q(i)$（这里 $i=\sqrt{-1}$）中来考虑方程$x^2-2py^2=-1$，有分解式

$$(x+i)(x-i)=(1-i)(1+i)(a+bi)(a-bi)y^2, \qquad (8)$$

其中$1\pm i, a\pm bi$均为$Q(i)$的素数。由于$Q(i)$的单位数为± 1，$\pm i$，且（$x+i$，$x-i$）$=1-i$（或$1+i$，但$1+i$与$1-i$相结合），故(8)给出

$$x+i=(1\pm i)(a\pm bi)(c+di)^2, \qquad (9)$$

或

$$-ix+1=(1\pm i)(a\pm bi)(c+di)^2, \qquad (10)$$

这里$y=c^2+d^2$，c，d一奇一偶。由$b-a\equiv\pm 3 \pmod 8$及$b+a\equiv\pm 3 \pmod 8$易知，(9)和(10)展开后均不可能。例如对(9)中的一个情形$x+i=(1+i)(a+bi)(c+di)^2$可化为

$$x+i=(a-b)(c^2-d^2)-2(a+b)cd+[(a+b)(c^2-d^2)+2(a-b)cd]i,$$

于是$(a+b)(c^2-d^2)+2(a-b)cd=1$。由$b-a\equiv\pm 3 \pmod 8$及$b+a\equiv\pm 3 \pmod 8$，知$\pm 3(c^2-d^2)\pm 6cd\equiv 1 \pmod 8$。由$c,d$一奇一偶知，此给出$\pm 3\equiv 1 \pmod 8$或$\pm 1\pm 4\equiv 1 \pmod 8$，而这不可能。证毕。

对于$D=p_1\cdots p_s$，$p_i(i=1,\cdots,s)$是不同的奇素数，我们有

定理 6 如果$s=2$或$2\nmid s$，$p_i\equiv 1 \pmod 4$ $(i=1,\cdots,s)$且对任意的$i\neq j$，（$1\leqslant i$，$j\leqslant s$）都有$\left(\frac{p_j}{p_i}\right)=-1$，则方程(7)有整数解。

证 $s=1$是熟知的结果，下设$s>1$，设$x_0+y_0\sqrt{D}$是Pell方程(2)的基本解，则由$x_0^2-Dy_0^2=1$知$2\nmid x_0$，$2\mid y_0$，于是

$$\left(\frac{x_0+1}{2}\right)\left(\frac{x_0-1}{2}\right)=D\left(\frac{y_0}{2}\right)^2,$$

故得出

$$\frac{x_0+1}{2}=D_1u^2,\frac{x_0-1}{2}=D_2v^2,\quad y_0=2uv,$$

这里$D=D_1D_2$。由前两式推出

$$D_1u^2-D_2v^2=1。\qquad (11)$$

如果$D_1=1$，则$u+v\sqrt{D}$是方程(2) 的一组解，但

$v=\frac{y_0}{2u}<y_0$，与$x_0+y_0\sqrt{D}$是(2) 的基本解矛盾，故

$D_1>1$。如果$D_2=1$，则 (11)给出方程(7) 有解。现在证明 $D_1>1$，$D_2>1$时方程(11)不成立。

在$s=2$时，由$D_1>1$，$D_2>1$知D_1，D_2都是一个素数，由假设$\left(\frac{p_2}{p_1}\right)=-1$知(11)不成立。而在$2\nmid s$，$s>1$时，$D_1$和$D_2$中必有一个含有奇数个素因子，不妨设 $D_1=p_{i_1}\cdots p_{i_t}$，$2\nmid t$，这里 $p_{i_j}\in\{p_1,\cdots,p_s\}(j=1,\cdots,t)$。由$D_2>1$，设$p|D_2$，$p\in\{p_1,\cdots,p_s\}$，则$\left(\frac{p_{i_j}}{p}\right)=-1(j=1,\cdots,t)$。

现对(11)取模p 得

$$(D_1u)^2\equiv D_1(\bmod p),$$

此给出

$$1=\left(\frac{D_1}{p}\right)=\prod_{j=1}^{t}\left(\frac{p_{i_j}}{p}\right)=(-1)^t=-1,$$

这不可能，这就证明了定理6。证毕。

Ⅱ． $M=\pm2$和$M=\pm4$，首先我们证明

定理 7 设p 是素数，如果丢番图方程

$$x^2 - Dy^2 = \pm p \tag{12}$$

有解，则当 $p \mid 2D$时有一个结合类；当 $p \nmid 2D$时有两个结合类。

证 1)首先证明，(12)最多只有一个解 $u_0 + v_0\sqrt{D}$，$u_0 \geqslant 0$满足(4)和(5)。为此，设(12)有两个不同的解

$u_0 + v_0\sqrt{D}$和$u_1 + v_1\sqrt{D}$($u_0 \geqslant 0$，$u_1 \geqslant 0$)满足(4)和(5)，因此$v_0 \geqslant 0$，$v_1 \geqslant 0$。由(12)知$v_0 \neq 0$，$v_1 \neq 0$，故$v_0 > 0$，$v_1 > 0$。由

$$u_0^2 - Dv_0^2 = \pm p,\quad u_1^2 - Dv_1^2 = \pm p$$

消去D，得$u_0^2 v_1^2 - u_1^2 v_0^2 = \pm p(v_1^2 - v_0^2)$，故推出

$$u_0 v_1 - u_1 v_0 \equiv 0 \pmod{p}, \tag{13}$$

或

$$u_0 v_1 + u_1 v_0 \equiv 0 \pmod{p}。 \tag{14}$$

另一方面，由

$$\begin{aligned} p^2 &= (u_0^2 - Dv_0^2)(u_1^2 - Dv_1^2) = (u_0 u_1 - Dv_0 v_1)^2 \\ &\quad - D(u_0 v_1 - u_1 v_0)^2 = (u_0 u_1 + Dv_0 v_1)^2 \\ &\quad - D(u_0 v_1 + u_1 v_0)^2, \end{aligned}$$

知，(13)和(14)分别给出

$$\left(\frac{u_0 u_1 - Dv_0 v_1}{p}\right)^2 - D\left(\frac{u_0 v_1 - u_1 v_0}{p}\right)^2 = 1,$$

$$\left(\frac{u_0 u_1 + Dv_0 v_1}{p}\right)^2 - D\left(\frac{u_0 v_1 + u_1 v_0}{p}\right)^2 = 1。$$

如果$u_0 v_1 \pm u_1 v_0 \neq 0$，则有

$$\left|\frac{u_0 v_1 \pm u_1 v_0}{p}\right| \geqslant y_0, \tag{15}$$

这里y_0满足$x_0 + y_0\sqrt{D}$是Pell方程(2)的基本解。但由

$u_0\geqslant 0$，$u_1\geqslant 0$，$v_0>0$，$v_1>0$及(4)和(5)式得

$$|u_0v_1\pm u_1v_0|\leqslant u_0v_1+u_1v_0<y_0p,$$

此与(15)式矛盾。

如果$u_0v_1\pm u_1v_0=0$,则容易推出$u_0+v_0\sqrt{D}=u_1+v_1\sqrt{D}$与假设不符。

2)设$u_0+v_0\sqrt{D}$是结合类K的基本解，则$-u_0+v_0\sqrt{D}$是$\overline{K}$的基本解。故由1)的结论知，方程(12)最多有两个结合类K和$\overline{K}$。现设$u+v\sqrt{D}\in K$，则$u-v\sqrt{D}\in\overline{K}$。如果$K=\overline{K}$，则由定理1知$u+v\sqrt{D}\sim u-v\sqrt{D}$的充要条件是

$$u^2+v^2D\equiv 0(\mathrm{mod}\,p),\quad 2uv\equiv 0(\mathrm{mod}\,p)。$$

由于$u^2-Dv^2=\pm p$，$p\nmid v$,故上式等价于

$$2D\equiv 0(\mathrm{mod}\,p),\quad 2u\equiv 0(\mathrm{mod}\,p)。$$

此又等价于$2D\equiv 0(\mathrm{mod}\,p)$，这就证明了定理7。证毕。

同样方法可证

定理 8 设p是奇素数，如果丢番图方程

$$x^2-Dy^2=\pm 2p$$

有解,则当$p\mid D$时有一个结合类；当$p\nmid D$时有两个结合类。

由定理7知，方程

$$x^2-Dy^2=\pm 2 \tag{16}$$

如果有解，则仅有一个结合类。设$u_0+v_0\sqrt{D}$是(16)的基本解，令$\frac{(u_0+v_0\sqrt{D})^2}{2}=u+v\sqrt{D}$，则$u^2-Dv^2=1$,故$u+v\sqrt{D}$是方程(2)的解。设方程(2)的基本解为$x_0+y_0\sqrt{D}$，则由定理2知

$$u+v\sqrt{D}=\frac{(u_0+v_0\sqrt{D})^2}{2}\leqslant x_0+y_0\sqrt{D},$$

故在$u>0$，$v>0$时$u+v\sqrt{D}=x_0+y_0\sqrt{D}$。因此除$x^2-2y^2=-2$外，由定理3知，方程(16)的全部整数解可表为

$$x+y\sqrt{D}=\pm(u_0+v_0\sqrt{D})\left[\frac{(u_0+v_0\sqrt{D})^2}{2}\right]^n$$

$$=\pm\frac{(u_0+v_0\sqrt{D})^{2n+1}}{2^n},\ n\in Z。$$

对于方程$x^2-Dy^2=\pm 4$，类似地讨论可得出第二章§6的Ⅲ、Ⅳ和Ⅴ的结论。

最后，对更为一般的二元二次丢番图方程

$$D_1x^2-D_2y^2=M,\ D_1>0,\ D_2>0, \qquad (17)$$

这里D_1，D_2以及$D=D_1D_2$均不是平方数。如果(17)有解，则(17)仅有有限个结合类。设$u_0\sqrt{D_1}+v_0\sqrt{D_2}$是某结合类$K$的基本解（这里概念的解释均同前），则方程(17)属于类K的全部解可表为

$$x\sqrt{D_1}+y\sqrt{D_2}=\pm(u_0\sqrt{D_1}+v_0\sqrt{D_2})(x_0+y_0\sqrt{D})^n,\ n\in Z,$$

这里$x_0+y_0\sqrt{D}$是Pell方程$x^2-Dy^2=1$ ($D=D_1D_2$)的基本解。由于(17)可化为$(D_1x)^2-Dy^2=D_1M$，故对(17)的讨论可归结到方程(1)上。

§4 方程 $x^2-Dy^2=M$ 的应用

Ⅰ. Gauss定理

首先证明Gauss对一般的二元二次丢番图方程的一个结果。

定理 1 对于丢番图方程

$$ax^2+bxy+cy^2+dx+ey+f=0, \tag{1}$$

设$D=b^2-4ac>0$，D不是平方数，$\Delta=4acf+bde-ae^2-cd^2-fb^2\neq0$。如果方程(1)有一组解，则必有无穷多组解。

证 由于D不是平方数，故$a\neq0$，不失一般可设$a>0$，由§1知，在变换

$$\begin{cases} X=2aDx+bDy+dD \\ Y=Dy-2ae+bd \end{cases} \tag{2}$$

下，方程(1)可化为

$$X^2-DY^2=M, \tag{3}$$

这里$M=4aD\Delta\neq0$。由于方程(1)有一组解，设为x_1, y_1，则得到(3)的一组解

$$\begin{cases} X_1=2aDx_1+bDy_1+dD, \\ Y_1=Dy_1-2ae+bd。 \end{cases} \tag{4}$$

因此，由§3的定理3知，方程(3)有无穷多组解。现在我们来证明，(3)存在无穷多组解通过变换(2)给出方程(1)的无穷多组解。

首先对$2aD^2$，Pell方程$x^2-Dy^2=1$存在无穷多个解$T_1+U_1\sqrt{D}$满足$U_1\equiv0(\bmod 2aD^2)$。这是因为对任意的$d>0$均使得方程$x^2-Dd^2y'^2=1$有无穷多组解x, y'。于是由$U_1\equiv0(\bmod 2aD^2)$推出$T_1^2\equiv1(\bmod 2aD^2)$。令

$T+U\sqrt{D}=(T_1+U_1\sqrt{D})^2$，则由

$$T+U\sqrt{D}=T_1^2+U_1^2D+2T_1U_1\sqrt{D},$$

推出$T\equiv1(\bmod 2aD^2)$，$U\equiv0(\bmod 2aD^2)$。于是由$x^2-Dy^2=1$的无穷多组解$T+U\sqrt{D}$得出方程(3)的无穷多组解

$$X+Y\sqrt{D}=(X_1+Y_1\sqrt{D})(T+U\sqrt{D})。\tag{5}$$

由(5)解出

$$X=X_1T+Y_1UD,\quad Y=X_1U+Y_1T,$$

故由(2)得

$$\begin{cases} X_1T+Y_1UD=2aDx+bDy+dD, \\ X_1U+Y_1T=Dy-2ae+bd。\end{cases}\tag{6}$$

我们来证明在$T\equiv 1(\bmod 2aD^2)$，$U\equiv 0(\bmod 2aD^2)$时，(6)给出的x，y是整数。为此对(6)取模$2aD^2$得

$$\begin{cases} X_1\equiv 2aDx+bDy+dD(\bmod 2aD^2), \\ Y_1\equiv Dy-2ae+bd(\bmod 2aD^2)。\end{cases}\tag{7}$$

把(4)代入(7)得

$$\begin{cases} 2aD(x-x_1)+bD(y-y_1)\equiv 0(\bmod 2aD^2), \\ D(y-y_1)\equiv 0(\bmod 2aD^2)。\end{cases}$$

由此推出$y-y_1\equiv 0(\bmod 2aD)$ 及$x-x_1+bD\dfrac{y-y_1}{2aD}\equiv 0(\bmod D)$，故由(6)决定的$x$,$y$是整数。于是,我们证明了,从(3)的无穷多组解$T\equiv 1(\bmod 2aD^2)$，$U\equiv 0$ $(\bmod 2aD^2)$通过变换(2)得到无穷多组方程(1)的解。证毕。

Ⅱ．幂数问题

方程 $x^2-Dy^2=M$ 的一些结果，还可以用来解决一些幂数问题。所谓幂数n是指,如果素数$p|n$，则$p^2|n$。1970年Golomb[2]证明了：1,4均可表为两个互素幂数之差，且表法无限。同时,Golomb 提出了如下两个问题和两个猜想：

1） 是否存在$4k-1$，$4k+1$形的连续奇幂数？

2） 除$12167=23^3$，$12168=2^3\cdot 3^2\cdot 13^2$外，是否还存在都不为平方数的连续奇幂数？

3） Golomb猜想(Ⅰ)：6不能表为两幂数之差。

4) Golomb猜想(Ⅱ)：存在无穷多个形如 $2(2a+1)$ $(a\geqslant 0)$的数不能表为两幂数的差。

1972年，Makowski[3]证明了素数$p\equiv 1(\mathrm{mod}8)$ 可表示为两个互素幂数的差，并且表法无限。1981年，Sentance[4]给出了无限多对形如$4k+1$，$4k+3$的连续奇幂数。1987年，肖戎[5]解决了Golomb 提出的两个问题和 猜想(Ⅰ)，即给出了问题1)和2)的肯定回答，否定了猜想(Ⅰ)。后者因为他找到了$6=5^4\cdot 7^3-463^2$的反例。

现在，我们利用方程 $x^2-Dy^2=M$ 的解的性质，给出Golomb猜想(Ⅱ)的一个否定回答，即有

定理 2 形如$2(2a+1)(a\geqslant 1)$的数均可表示为两个互素幂数之差，且表法无限。

证 设$2(2a+1)=2b$，$b>1$。取$k_0=\frac{(b-1)^2}{2}-1$,则有

$2\nmid k_0$,$(k_0,b)=1$。令$D=(b+k_0)^2-b^2=\left(\frac{b^2-3}{2}\right)^2-2>0$

(因为$b>1$)，显然D非平方数，且Pell方程$x^2-Dy^2=1$的基本解为$\left(\frac{b^2-3}{2}\right)^2-1+\frac{b^2-3}{2}\sqrt{D}$。由于方程$x^2-Dy^2=b^2$有解 $b+k_0+\sqrt{D}$，故在与$b+k_0+\sqrt{D}$相结合的类中，方程 $x^2-Dy^2=b^2$ 的全部正整数解（见§3的定理3）可表为

$$x_n+y_n\sqrt{D}=(b+k_0+\sqrt{D})(x_0+y_0\sqrt{D})^n,n>0,\quad (8)$$

其中 $x_0=\left(\frac{b^2-3}{2}\right)^2-1$，$y_0=\frac{b^2-3}{2}$。我们来证明，(8)中存在无穷多个$n$满足$2|x_n$，$(x_n,b)=1$且$D|y_n$。

①当$n\equiv 0(\mathrm{mod}2)$时(8)给出$2|x_n$。这是因为 $2\nmid bk_0$，对(8)取模 2知 $x_n+y_n\sqrt{D}\equiv\sqrt{D}(\mathrm{mod}2)$，故$2|x_n$。

②对任意$n>0$，均有$(x_n, b)=1$。因为$D\equiv k_0^2 \pmod b$，故对$x_0^2-Dy_0^2=1$取模b得

$$(x_0+k_0y)(x_0-k_0y)\equiv 1 \pmod b。\qquad (9)$$

现对(8)取模b得

$$x_n+y_n\sqrt{D}\equiv(k_0+\sqrt{D})(x_0+y_0k_0)^n \pmod b,$$

注意到(9)式知，上式给出

$$(x_n,b)=(b,k_0(x_0+y_0k_0)^n)=(b,k_0)=1。$$

③由存在正整数n_1，凡$n\equiv n_1 \pmod D$都有$D|y_n$。这是因为对(8)取模D得

$$x_n+y_n\sqrt{D}\equiv(b+k_0+\sqrt{D})(x_0^n+nx_0^{n-1}y_0\sqrt{D}) \pmod D$$
$$\equiv x_0^n(b+k_0)+x_0^{n-1}[x_0+ny_0(b+k_0)]\sqrt{D} \pmod D,$$

由此知

$$y_n\equiv x_0^{n-1}[x_0+ny_0(b+k_0)] \pmod D。\qquad (10)$$

由于$(y_0,D)=1$，$(b+k_0,D)=(b+k_0,bk_0)=1$，故关于n的一次同余式$x_0+ny_0(b+k_0)\equiv 0 \pmod D$有解$n_1$，$0<n_1<D$。于是对满足$n\equiv n_1 \pmod D$的$n$，(10)给出$D|y_n$。

由①～③即知，(8)式中有无穷多个n满足$2|x_n$，$(b,x_n)=1$且$D|y_n$。对于这些n，令$y_n=Dy_n'$，则由$x_n^2-Dy_n^2=b^2$知

$$(x_n+b)(x_n-b)=D(Dy_n')^2=D^3y_n'^2。\qquad (11)$$

由$2|x_n$，$(b,x_n)=1$知$(x_n+b, x_n-b)=1$，故从(11)知，存在正整数u，v_n，s，t_n使得

$$x_n+b=u^3v_n^2,\quad x_n-b=s^3t_n^2,\qquad (12)$$

其中$D=us$，$y_n'=v_nt_n$，且$(uv_n, st_n)=1$。由(12)即知

$$2b=u^3v_n^2-s^3t_n^2,$$

这就表明了$2b(b=2a+1>1)$可表为两个互素幂数之差，且表法无限。证毕。

定理2的证明是构造性的，例如我们下面给出6表为无穷多组两个互素幂数之差的方法。

在定理2的证明中，取$b=3$，则$k_0=1$，$D=7$且Pell方程$x^2-7y^2=1$的基本解$x_0+y_0\sqrt{7}=8+3\sqrt{7}$。由于方程$x^2-7y^2=9$有解$4+\sqrt{7}$，故在与$4+\sqrt{7}$相结合的类中，方程$x^2-7y^2=9$的全部正整数解可表为

$$x_n+y_n\sqrt{7}=(4+\sqrt{7})(8+3\sqrt{7})^n, n>0。$$

现在求出满足$2|x_n$，$(x_n, 3)=1$且$7|y_n$的n。由①～③知，满足这些条件的$n\equiv 0(\mathrm{mod}2)$且$8+n\cdot 3(3+1)\equiv 0(\mathrm{mod}7)$，故$n\equiv 4(\mathrm{mod}14)$，于是

$$6=u^3v_n^2-s^3t_n^2, \tag{13}$$

这里$us=7$，$7v_nt_n=y_n$。例如取$n=4$，则$y_4=81025=7\cdot 5^2\cdot 463$。故由$us=7$，$v_4t_4=5^2\cdot 463$知(13)给出

$$6=5^4\cdot 7^3-463^2。$$

对于2表为两幂数差的问题，从Pell方程$x^2-Dy^2=1$可十分容易地构造出来。例如，类似于定理2的证明，取k_0为任意的正奇数，$D=(k_0+1)^2-1$，则Pell方程$x^2-Dy^2=1$的全部正整数解可表为

$$x_n+y_n\sqrt{D}=(k_0+1+\sqrt{D})^n。$$

在$n\equiv D(\mathrm{mod}2D)$时，上式给出$2|x_n$，$D|y_n$，故从$x_n^2-1=Dy_n^2=D^3y_n'^2$可推出2是无穷多个两幂数之差。

类似地可证[6]：任意正整数都可表为两互素幂数之差，且表法无限。

§5 两个三元二次丢番图方程的公解

求两个三元二次丢番图方程的公解问题引人注目。所谓

求两个三元二次丢番图方程的公解问题，是指求丢番图方程组

$$\begin{cases} x^2 - Dy^2 = k \\ y^2 - D_1 z^2 = m \end{cases} \tag{1}$$

的整数解，这里D，D_1，k和m都是给定的整数，$D>0$，$D_1>0$都不是平方数。利用Baker有效方法，可以定出(1)中$|y|$的上界，因此方程(1)最多只有有限个解（参阅第三章§4）。

1941年，Ljunggren[7]证明了

定理 1 Pell方程组

$$\begin{cases} x^2 - 2y^2 = 1 \\ y^2 - 3z^2 = 1 \end{cases}$$

仅有正整数解$x=3$，$y=2$，$z=1$。

我们在第三章的§4给出了定理1用Baker方法的证明。1969年，Baker和Davenport[8]利用Baker方法证明了

定理 2 丢番图方程组

$$\begin{cases} y^2 - 3x^2 = -2 \\ z^2 - 8x^2 = -7 \end{cases}$$

仅有两组正整数解$x=y=z=1$和$x=11$，$y=19$，$z=31$。

1975年，Kanagasabapathy和Ponnudurai[9]用递推序列的方法给出了定理2的一个初等证明。1980年，Velupillai[10]证明了

定理 3 丢番图方程组

$$\begin{cases} z^2 - 3y^2 = -2 \\ z^2 - 6x^2 = -5 \end{cases}$$

仅有正整数解$x=y=z=1$和$x=29$，$y=41$，$z=71$。

1983年，曹珍富[11]用Pell方程的方法，研究了较为一般的Pell方程组

$$\begin{cases} x^2-2y^2=-1 \\ y^2-Dz^2=1 \end{cases} \tag{2}$$

的正整数解。证明了

定理 4 设$D=p_1\cdots p_s$，$p_i(i=1,\cdots,s)$是不同的奇素数，$1\leqslant s\leqslant 5$ 则Pell 方程组(2)除开$s=4$时，仅有正整数解$x=239$，$y=169$，$z=4$（当$D=3\cdot5\cdot7\cdot17=1785$）和$x=1393$，$y=985$，$z=4$（当$D=3\cdot17\cdot41\cdot29=60639$）外，无其它的正整数解。

证 由$x^2-2y^2=-1$解出

$$x=\frac{\delta^{2n+1}+\bar{\delta}^{2n+1}}{2},\quad n>0,$$

这里$\delta=1+\sqrt{2}$，$\bar{\delta}=1-\sqrt{2}$。记

$$\xi_n=\frac{\delta^n+\bar{\delta}^n}{2},\qquad \eta_n=\frac{\delta^n-\bar{\delta}^n}{2\sqrt{2}},$$

则我们有

$$x+1=\xi_{2n+1}+1=\begin{cases} 2\xi_{2m}\xi_{2m+1}, & 当n=2m; \\ 4\eta_{2m+2}\eta_{2m+1}, & 当n=2m+1。\end{cases}$$

$$x-1=\xi_{2n+1}-1=\begin{cases} 4\eta_{2m}\eta_{2m+1}, & 当n=2m; \\ 2\xi_{2m+2}\xi_{2m+1}, & 当n=2m+1。\end{cases}$$

故从(2)得出$x^2-1=2Dz^2$，从而知道

$$\xi_{(2m+1)\pm1}\cdot\xi_{2m+1}=D_1z_1^2,\quad \eta_{(2m+1)\pm1}\cdot\eta_{2m+1}=D_2z_2^2, \tag{3}$$

这里$D=D_1D_2$，$z=2z_1z_2$。由于

$$(\xi_{(2m+1)\pm1},\ \xi_{2m+1})=1,\quad (\eta_{(2m+1)\pm1},\ \eta_{2m+1})=1,$$

故(3)式给出

$$\xi_{(2m+1)\pm1}=ka^2,\quad \xi_{2m+1}=lb^2,\quad \eta_{(2m+1)\pm1}=ec^2,$$
$$\eta_{2m+1}=fd^2, \tag{4}$$

这里$D_1=kl$，$z_1=ab$；$D_2=ef$，$z_2=cd$。由于

$$\xi^2_{(2m+1)\pm1}-2\eta^2_{(2m+1)\pm1}=1,\ \xi^2_{2m+1}-2\eta^2_{2m+1}=-1,$$

故(4)式给出

$$k^2a^4-2e^2c^4=1,\ l^2b^4-2f^2d^4=-1。\tag{5}$$

由于k,e,l,f等于1时，方程(5)分别化为方程$X^4-2Y^2=1$，$X^2-2Y^4=1$，$X^4-2Y^2=-1$和$X^2-2Y^4=-1$，而这些方程都已经给出了全部解(见第二章§2、§3和§7)，故在$1\leqslant s\leqslant 3$时，定理4得到了证明。在$s\geqslant 4$时，设$k>1$，$e>1$，$l>1$，$f>1$，由(5)的第一式知

$$ka^2\pm1=4u^2,\ ka^2\mp1=2v^2,\ 2uv=ec^2。\tag{6}$$

由(6)的前两式知$v^2-2u^2=\mp1$。由$2uv=ec^2$知$2|u$，故$v^2-2u^2=\mp1$中的负号不可能。于是(6)给出

$$v^2-2u^2=1,\ 2uv=ec^2。$$

由$2uv=ec^2$得$u=2e_1u_1^2$，$v=e_2v_1^2$，$c=u_1v_1$，$e=e_1e_2$ 代入$v^2-2u^2=1$得出

$$e_2^2v_1^4-8e_1^2u_1^4=1,\tag{7}$$

由于$e_1=1,e_2=1$上式分别化为$X^2-8Y^4=1$及$X^4-8Y^2=1$,而这些方程也已在第二章解决，故经过一些计算知，定理4成立。

下设$e_1>1$，$e_2>1$，故由$D=klef=kle_1e_2f$知 $s\geqslant5$且在$s=5$时，可设k，l，e_1,e_2，f均是一个素数。于是由(7)得出

$$e_2v_1^2\pm1=4u_2^2,\ e_2v_1^2\mp1=2u_3^2,\ u_2u_3=e_1u_1^2,\tag{8}$$

由$u_2u_3=e_1u_1^2$得出$u_2=e_1u_4^2$，$u_3=u_5^2$或$u_2=u_4^2$，$u_3=e_1u_5^2$，故由(8)的前两式得出

$$u_5^4-2(e_1u_4^2)^2=\mp1或(e_1u_5^2)^2-2u_4^4=\mp1。$$

而这些方程均已解决，用这些方程的解不断回代，最后得证定理4的论断。证毕。

利用这种方法还可以考虑$D=p_1\cdots p_s$及$D=2p_1\cdots p_s$，这里$p_i(i=1,\cdots s)$是不同的奇素数的一般情形[11]。由于(2)给出$x^2+1=2y^2$，$x^2-1=2Dz^2$，推出$x^4-1=D(2yz)^2$。故(2)的解可以应用到二元四次丢番图方程$x^4-Dy^2=1$上去（参阅第七章§1)。

关于两个Pell方程的公解问题，1984年Mohanty和Ramasamy[12]用递推序列的方法还证明了

定理 5 Pell方程组

$$\begin{cases} x^2-2y^2=1 \\ y^2-5z^2=4 \end{cases} \tag{9}$$

仅有$x=\pm 3$，$y=\pm 2$，$z=0$的整数解。

证 利用Pell 方程的解知，方程$x^2-2y^2=1$的全部解可表为

$$x_n+y_n\sqrt{2}=(3+2\sqrt{2})^n,\quad n\in Z。$$

由此得到一组关系式

$$x_{-n}=x_n,\quad y_{-n}=-y_n, \tag{10}$$

$$x_{n+r}=x_nx_r+2y_ny_r, \tag{11}$$

$$y_{n+r}=x_ny_r+x_ry_n, \tag{12}$$

$$x_{2n}=x_n^2+2y_n^2=2x_n^2-1=4y_n^2+1, \tag{13}$$

$$y_{2n}=2x_ny_n, \tag{14}$$

$$x_{5n}=x_n(16x_n^4-20x_n^2+5), \tag{15}$$

$$y_{5n}=y_n(16x_n^4-12x_n^2+1), \tag{16}$$

$$y_{n+2r}\equiv -y_n(\bmod x_r), \tag{17}$$

$$y_{n+2(r+1)}\equiv y_n(\bmod 2x_r+3y_r), \tag{18}$$

$$y_{n+2(r+1)}\equiv -y_n(\bmod 3x_r+4y_r)。 \tag{19}$$

通过计算可得下列的数据：

n	x_n	y_n
0	1	0
1	3	2
2	17	12
3	99	70
4	577	408
5	3363	2378
6	19601	13860
7	114243	80782
8	665857	470832
9	3880399	2744210
10	22619537	15994428

现在，设(9)存在整数解，令$5z=\lambda$，则由$y_n^2-5z^2=4$得出

$$\lambda^2=5y_n^2-20。\qquad (20)$$

我们利用$x^2-2y^2=1$的解的性质分五种情形来证明在$n\neq\pm1$时(20)不成立。

(a)从(18)，$y_{n+8}\equiv y_n(\bmod 2x_3+3y_3)\equiv y_n(\bmod 408)$

$$\equiv y_n(\bmod 17),$$

如果$n\equiv0$，$4(\bmod 8)$，则$y_n\equiv\left\{\begin{matrix} y_0,当n\equiv0(\bmod 8) \\ y_4,当n\equiv4(\bmod 8)\end{matrix}\right\}\equiv$ $0(\bmod 17)$，对(20)取模17知

$$1=\left(\frac{5y_n^2-20}{17}\right)=\left(\frac{-3}{17}\right)=\left(\frac{-1}{17}\right)\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

这不可能。如果$n\equiv\pm2(\bmod 8)$，则$y_n\equiv y_{\pm2}=\pm y_2=$ $\pm12(\bmod 17)$，故对(20)取模17给出 $1=\left(\frac{5\cdot12^2-3}{17}\right)=$ $\left(\frac{3}{17}\right)=-1$，也不可能。这就证明了$n\equiv0(\bmod 2)$时(20)不成立。

(b)利用(12)，$y_{n+5}=2378x_n+3363y_n\equiv y_n(\bmod 41)$。故在$n\equiv\pm2(\bmod 5)$时，$y_n\equiv y_{\pm2}=\pm12(\bmod 41)$，对(20)取模41得

$$1=\left(\frac{5y_n^2-20}{41}\right)=\left(\frac{5\cdot12^2-20}{41}\right)=\left(\frac{3}{41}\right)=-1,$$

这不可能。这就证明$n\equiv\pm2(\bmod 5)$时(20)不成立。

(c)利用(19)，$y_{n+20}\equiv-y_n(\bmod 3x_9+4y_9)\equiv-y_n(\bmod 22619537)\equiv-y_n(\bmod 241)$，这给出$y_{n+40}\equiv y_n(\bmod 241)$。如果$n\equiv\pm5(\bmod 40)$，则$y_n\equiv\mp32(\bmod 241)$，故对(20)取模241得

$$1=\left(\frac{5y_n^2-20}{241}\right)=\left(\frac{5\cdot32^2-20}{241}\right)=\left(\frac{39}{241}\right)=-1,$$

这不可能。

如果 $n\equiv\pm9(\bmod 40)$，则 $y_n\equiv\mp57(\bmod 241)$，因此(20)给出

$$1=\left(\frac{5y_n^2-20}{241}\right)=\left(\frac{5\cdot57^2-20}{241}\right)=\left(\frac{78}{241}\right)=-1;$$

如果$n\equiv\pm11(\bmod 40)$，则$y_n\equiv\mp57(\bmod 241)$；如果$n\equiv\pm15(\bmod 40)$，则$y_n\equiv\mp32(\bmod 241)$，同前证明知，(20)此时均不成立。这就证明$n\equiv\pm5$，$\pm9$，$\pm11$，$\pm15(\bmod 40)$时方程(20)不成立。

由(a)、(b)和(c)知，除$n\equiv1,19,21,39(\bmod 40)$即$n\equiv1,19(\bmod 20)$外，其余情形方程(20)均不成立。

(d)如果$n\equiv1(\bmod 20)$，$n\neq1$，可设$n=1+5\cdot2^t(2h+1)$，$h\geqslant0$和$t\geqslant2$。令$j=2^t$，$t\geqslant2$，我们有 $n=5j+1+2\cdot5j\cdot h$。利用(17)式我们有

$$y_n\equiv(-1)^h y_{5j+1}(\bmod x_{5j})\equiv(-1)^h x_1 y_{5j}(\bmod x_{5j})$$

$\equiv(-1)^{h}3y_j(16x_j^4-12x_j^2+1)(\bmod x_j(16x_j^4-20x_j^2+5))$。故对(20)取模$x_j$得

$$1=\left(\frac{5(3y_j)^2-20}{x_j}\right)=\left(\frac{45y_j^2-20}{x_j}\right)。$$

由于$x_j^2-2y_j^2=1$，故$-20\equiv 40y_j^2(\bmod x_j)$。因此上式给出

$$1=\left(\frac{45y_j^2+40y_j^2}{x_j}\right)=\left(\frac{85}{x_j}\right)=\left(\frac{5}{x_j}\right)\left(\frac{17}{x_j}\right), \qquad (21)$$

由归纳法，容易知道，对$t\geqslant 1$，有

$$x_j\equiv 1(\bmod 4),\quad x_j\equiv 2(\bmod 5),$$

且$t=2$时$x_j\equiv -1(\bmod 17)$，$t\geqslant 3$时$x_j\equiv 1(\bmod 17)$。故在$t=2$时，(21)给出

$$1=\left(\frac{x_j}{5}\right)\left(\frac{x_j}{17}\right)=\left(\frac{2}{5}\right)\left(\frac{-1}{17}\right)=-1,$$

而在$t\geqslant 3$时，(21)给出

$$1=\left(\frac{2}{5}\right)\left(\frac{1}{17}\right)=-1,$$

因此$n\equiv 1(\bmod 20)$，$n\neq 1$时方程(20)不成立。

(e)如果$n\equiv 19(\bmod 20)$，则$n\equiv -1(\bmod 20)$。故注意到(10)式，同(d)的证明可知$n\neq -1$时方程(20)不成立。

由(a)～(e)知，(20)有解推出$n=\pm 1$，$y=\pm 2$，于是给出$x=\pm 3$，$z=0$。证毕。

曹珍富[13],[14]发现，Pell方程组(9)不用较麻烦的递推序列方法，而用Pell方程的技巧可给出一个非常简短的证明，而且此方法可适用于一般的Pell方程组

$$\begin{cases} x^2-2y^2=1, \\ y^2-Dz^2=4。\end{cases} \qquad (22)$$

我们有

定理 6 设 $p_1,\cdots,p_s$是不同的奇素数，则当 $D=p_1\cdots p_s\equiv 1(\bmod 4),1\leqslant s\leqslant 4$时方程组(22)仅有平凡解$z=0$。

定理 7 设$p_1,\cdots,p_s$是不同的奇素数，则当$D=2p_1\cdots p_s$，$1\leqslant s\leqslant 4$ 时方程组(22)除开$D=34$ 仅有非平凡解$z=\pm 12$外，均只有平凡解$z=0$。

下面给出定理6和7的证明思路。由方程 $x^2-2y^2=1$ 可知 $y=\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{2}}$，$n\in Z$,这里$\varepsilon=3+2\sqrt{2}$，$\bar{\varepsilon}=3-2\sqrt{2}$。

把 $y=\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{2}}$ 代入$y^2-Dz^2=4$可得

$$\left(\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{2}}-2\right)\left(\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{2}}+2\right)=Dz^2。\tag{23}$$

由于在$D\equiv 1(\bmod 4)$或$D\equiv 0(\bmod 2)$时，(22)给出$2\|y$，故由 $y=\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{2}}$知$2\nmid n$。令$n=2m+1$，则(23)给出

$$\frac{\varepsilon^{2m+1}-\bar{\varepsilon}^{2m+1}}{2\sqrt{2}}-2=4D_1z_1^2,\quad \frac{\varepsilon^{2m+1}-\bar{\varepsilon}^{2m+1}}{2\sqrt{2}}+2=4D_2z_2^2,\tag{24}$$

这里$D=D_1D_2$，$z=4z_1z_2$。由于

$$\frac{\varepsilon^{2m+1}-\bar{\varepsilon}^{2m+1}}{2\sqrt{2}}-2=(\varepsilon^{m+1}+\bar{\varepsilon}^{m+1})\left(\frac{\varepsilon^m-\bar{\varepsilon}^m}{2\sqrt{2}}\right),$$

$$\frac{\varepsilon^{2m+1}-\bar{\varepsilon}^{2m+1}}{2\sqrt{2}}+2=(\varepsilon^m+\bar{\varepsilon}^m)\left(\frac{\varepsilon^{m+1}-\bar{\varepsilon}^{m+1}}{2\sqrt{2}}\right),$$

故(24)可化为

$$\left(\frac{\varepsilon^{m+1}+\bar{\varepsilon}^{m+1}}{2}\right)\left(\frac{\varepsilon^m-\bar{\varepsilon}^m}{2\sqrt{2}}\right)=2D_1z_1^2,\tag{25}$$

$$\left(\frac{\varepsilon^m+\bar{\varepsilon}^m}{2}\right)\left(\frac{\varepsilon^{m+1}-\bar{\varepsilon}^{m+1}}{2\sqrt{2}}\right)=2D_2z_2^2。\qquad (26)$$

由于$\varepsilon=3+2\sqrt{2}=\rho^2$，$\rho=1+\sqrt{2}$，故对任意$k$，$\dfrac{\varepsilon^k-\bar{\varepsilon}^k}{2\sqrt{2}}$可分解为 $2\left(\dfrac{\rho^k+\bar{\rho}^k}{2}\right)\left(\dfrac{\rho^k-\bar{\rho}^k}{2\sqrt{2}}\right)$，故从(25)和(26)经过一些讨论就可证明定理6和定理7。

用这个方法，还可以解决(22)中$D=p_1\cdots p_s(\equiv1(\mathrm{mod}\,4))$或$2p_1\cdots p_s$当$s\leqslant6$时的情形。

最后，我们给出Ljunggren对于丢番图方程组

$$\begin{cases} x^2+(x+1)^2=z \\ y^2+(y+1)^2=z^2 \end{cases}\qquad (27)$$

和

$$\begin{cases} |Mx^2-N|=z \\ z^2=My^2-N \end{cases}\qquad (28)$$

的结果，即有

定理 8[15] 丢番图方程组(27)仅有正整数解$x=1$，$y=3$，$z=5$。

定理 9[16] 设$N>1$，则丢番图方程组(28)仅有非负整数解$x=0$，$y=1$，$z=N$(当$M=N(N+1)$)和$x=2$，$y=4N+1$，$z=|4M-N|$(当$M=N(N+1)$或$N=16M$)。

在Ljunggren之前，Trost[17]曾解决方程(28)当$M=N(N+1)$，$N=D^2(D\mp1)$时的特殊情形。

§6 三元以上的二次丢番图方程

Ⅰ. Legendre方程及其应用

三元二次丢番图方程的最著名的例子是Legendre 方程

$$ax^2+by^2+cz^2=0, \tag{1}$$

这里$abc\neq 0$，a,b,c 都无平方因子，两两互素且符号不全一样。Legendre证明了

定理 1 方程(1)有不全为零的解的充要条件是：$-bc$，$-ac$，$-ab$分别是模$|a|$，$|b|$，$|c|$的二次剩余。

这个定理的必要性易证。设(1)有一组不全为零的解x，y，z，则不妨设$(x,y,z)=1$。于是，若有素数 $p|a$，必有$p\nmid z$(否则由$p|a$，$p|z$推出$p|y$，再由$p|y$，$p|z$推出$p|x$)，所以对(1)式取模$|a|$知

$$(bz^{-1}y)^2\equiv -bc(\bmod |a|)$$

故$-bc$是$|a|$的二次剩余。同理可证$-ac$，$-ab$分别是模$|b|$，$|c|$的二次剩余。

应该指出，这个定理的充分性远不是显然的。但由于介绍这个证明的书籍较多（可参看[18]），故这里从略。

方程(1)的一些特例，如方程 $x^2+y^2=z^2$，$x^2+py^2=z^2$以及 $x^2+y^2=pz^2$（p为素数）等都可以给出它们的全部解。我们在第二章的§2给出了方程$x^2+y^2=z^2$及$x^2+2y^2=z^2$的全部解，现在我们给出方程

$$x^2+y^2=2z^2,\ (x,\ y)=1 \tag{2}$$

的全部正整数解。由(2)显然，$x\equiv y\equiv 1(\mathrm{mod}\,2)$。故除$x=y$外，可令$x+y=2u$，$x-y=2v$，这里 $u>0,v>0$。于是 $x=u+v$，$y=u-v$。代入(2)得

$$u^2+v^2=z^2。$$

由于$(x,y)=1$，故$(u,v)=(x,y)=1$。所以上式给出

$$u=2ab,\ v=a^2-b^2,\ z=a^2+b^2,$$

(u,v可交换）这里$a>b>0$，$(a,b)=1$且a，b一奇一偶。于

是得到方程(2)除$x=y$外的全部正整数解为

$$x=2ab+a^2-b^2,\quad y=|2ab-a^2+b^2|,\quad z=a^2+b^2,$$

（x,y可交换）这里$a>b>0$，$(a,b)=1$且a,b一奇一偶。

Legendre方程在组合数学中有其重要应用。设A是v个元素$a_1,\cdots,a_v$的集合（称为v—集），$A_1,\cdots,A_v$是A的v个子集。如果$A_i(i=1,\cdots,v)$满足条件：

1） 每个A_i是A的k—子集；

2） 任给的$i\neq j$，$A_i\cap A_j$是A的λ—子集；

3） 整数v,k,λ满足$0<\lambda<k<v-1$。

则称子集$A_1,\cdots,A_v$为A的一个（v,k,λ）—组态（在统计学中，（v,k,λ)—组态称为对称平衡不完全区组设计）。

从定义容易知道，v,k,λ满足

$$k-\lambda=k^2-\lambda v。\tag{3}$$

由组合数学[19]知：设v,k,λ 是整数，如果存在(v,k,λ)—组态，则当v是偶数时，$k-\lambda$ 是平方数；当v是奇数时，丢番图方程

$$x^2=(k-\lambda)y^2+(-1)^{\frac{v-1}{2}}\lambda z^2\tag{4}$$

必有x,y,z不全为零的整数解。

定理 2 设$2\nmid v$，$(k,\lambda)=1$，如果存在(v,k,λ)—组态，则 $(-1)^{\frac{v-1}{2}}\lambda$是$l$的二次剩余，这里$l$是$k-\lambda$的无平方因子部分。

证 当$2\nmid v$时，存在(v,k,λ)—组态的必要条件是(4)有一组x,y,z不全为零的整数解。由于$(k,\lambda)=1$，故$(k-\lambda,\lambda)=1$。设$k-\lambda=l\xi^2$，$\lambda=d\eta^2$，这里l,d均为无平方因子的正整数，则由定理1知，方程(4)有一组不全为零的解推出$l,(-1)^{\frac{v-1}{2}}d$分别是模d，l的二次剩余。现在由(3)知$k^2=$

$(k-\lambda)+\lambda v\equiv l\xi^2 \pmod d$，故由$(d,k)=1$知$l$是模$d$的二次剩余。于是推出 $(-1)^{\frac{v-1}{2}}d$是模l的二次剩余，即 $(-1)^{\frac{v-1}{2}}\lambda$是模$l$的二次剩余。证毕。

这个定理的一个推论是给出不存在某些参数为$v=n^2+n+1$，$k=n+1$，$\lambda=1$的(v,k,λ)一组态（此时的(v,k,λ)一组态称为n阶有限射影平面）。

推论 设$n\equiv 1 \pmod 4$或$n\equiv 2 \pmod 4$，且n的无平方因子部分至少有一个素因子是$4k+3$形的，则参数为$v=n^2+n+1$，$k=n+1$，$\lambda=1$的(v,k,λ)—组态不存在。

证 在$n\equiv 1 \pmod 4$或$n\equiv 2 \pmod 4$时，$\frac{v-1}{2}$是奇数。故由定理2知-1是模l的二次剩余，这里l是 $k-\lambda=n$的无平方因子部分。但由假设至少存在素数 $p\equiv 3 \pmod 4$，$p\mid l$，而 $\left(\frac{-1}{p}\right)=-1$，故不存在参数为 $v=n^2+n+1$，$k=n+1$，$\lambda=1$的(v,k,λ)—组态。

Ⅱ. 丢番图方程 $ax^2+by^2+cz^2=n$

现在我们来讨论Legendre方程的推广形式：

$$ax^2+by^2+cz^2=n,\quad n\neq 0。\tag{5}$$

裴定一[26]给出了方程(5)的解的个数表达式。对于a,b,c的一些特殊值，我们还有以下熟知的结果。

定理 3 设 $(a,b,c)=(1,1,1)$，则当 $n=4^\lambda(8\mu+7)$，$\lambda\geqslant 0$，$\mu\geqslant 0$时(5)无解；而当n不具有形式$4^\lambda(8\mu+7)$时(5)有解。

当$(a,b,c)=(1,1,-1)$时，Erdös曾提出一个问题：是否对充分大的正整数n，都有整数x,y，z存在，使得

$$n=x^2+y^2-z^2,\quad x^2\leqslant n,\quad y^2\leqslant n,\quad z^2\leqslant n。\tag{6}$$

这个问题至今也未解决。但是，柯召[20]曾得出一系列有趣的结果。例如他证明了"几乎所有"的正整数n都满足(6)，即有

定理 4 设$A(N)$是小于N且不能表为(6)的形状的正整数n的个数，则有

$$A(N)=O\left(\frac{N}{\log N}\right)。$$

曹珍富发现，这个结果可以改进为$A(N)=O\left(\frac{\sqrt{N}}{\log N}\right)$。

证 设 $$a^2\leqslant n=a^2+b<(a+1)^2。$$

如果$4|b$，设$b=4m$，则有

$$n=a^2+(m+1)^2-(m-1)^2,$$

且显然$a^2\leqslant n$，$(m+1)^2\leqslant n$，$(m-1)^2\leqslant n$。如果$2\nmid b$，设$b=2m+1$，则有

$$n=a^2+(m+1)^2-m^2,\quad a^2\leqslant n,\quad (m+1)^2\leqslant n,\quad m^2\leqslant n。$$

如果$a\geqslant 4$，$b=4m+2$且有正整数k，l存在，使得

$$2a+4m+1=kl,\quad k>1,\quad l>1,$$

则有

$$n=(a-1)^2+\left(\frac{k+l}{2}\right)^2-\left(\frac{k-l}{2}\right)^2。$$

从$3k\leqslant lk=2a+4m+1$知$k-3\leqslant\frac{2a+4m+1}{3k}(k-3)=(2a+4m+1)\left(\frac{1}{3}-\frac{1}{k}\right)$。所以有$k+\frac{2a+4m+1}{k}\leqslant 3+\frac{2a+4m+1}{3}$。故在$a\geqslant 4$时得出

$$\left(\frac{k+l}{2}\right)^2=\left[\frac{1}{2}\left(k+\frac{2a+4m+1}{k}\right)\right]^2\leqslant\left[\frac{1}{2}\left(3+\frac{2a+4m+1}{3}\right)\right]^2$$

$$=\left[\frac{1}{3}(a+2m+5)\right]^2\leqslant n。$$

因此在$a\geqslant 4$时只有

$$n=a^2+4m+2,\quad 1\leqslant 2m+1\leqslant a, \tag{7}$$

而且

$$2a+4m+1=p\text{为素数} \tag{8}$$

时，才有可能不适合(6)式，于是得到

$$A(N)\leqslant\sum_{a=1}^{[\sqrt{N}]}\sum_{2a+4m+1=p}1\leqslant\sum_{a=1}^{[\sqrt{N}]}[\pi(4a)-\pi(2a)]$$

$$=\pi(4[\sqrt{N}])-1, \tag{9}$$

这里$\pi(x)$表示不超过x的素数个数。由初等数论中熟知的结论：$\pi(n)<12\frac{n}{\log n}$（当$n>1$）知，(9)给出

$$A(N)\leqslant 12\frac{4[\sqrt{N}]}{\log 4[\sqrt{N}]}=O\left(\frac{\sqrt{N}}{\log N}\right)\text{。证毕。}$$

柯召同时还讨论了n适合(7)、(8)时表为(6)的形状的可能性。

定理 5 如果存在奇数$t>1$使得整数m适合

$$\frac{a}{t}-\frac{1}{2}\geqslant m\geqslant\frac{a}{t+1}-\frac{1}{2}+\frac{1}{t^2+1},$$

则(7)中的数n可表为(6)的形状。

定理 6 (7)中数能表为(6)的形状的充要条件是：存在整数s和b_s使得

$$a+\sqrt{(a-2s-1)^2-4m-2}\geqslant b_s\geqslant a-\sqrt{(a-2s-1)^2-4m-2},\quad 0\leqslant s<\frac{a-1-\sqrt{4m+2}}{2},$$

且

$2(2s+1)a+4m+2-(2s+1)^2=b_sc_s$，这里$c_s$是正整数。

推论 $n=a^2+2$ 能表为(6)的形状的充要条件是存在整数$u\geqslant 1$，$v\geqslant 1$，$\frac{a-2}{2}\geqslant s\geqslant 0$使得$2(2s+1)a+2-(2s+1)^2=(1+2s+2u)(1+2s+2v)$。

此外，柯召通过计算发现，在$n\leqslant 10^4$时有76个数不能表为(6)的形状。其中最小的一个是3，最大的一个是6563。柯召猜测：

"充分大的正整数都能表为(6)的形状。6563 很可能是不能表为(6)的最大整数"。

即使对于a^2+2，要证明a充分大时，a^2+2均能表为(6)的形状亦很困难。

Ⅲ。最后，对于四元二次型

$$f=f(x,y,z,w)=x^2+bcy^2+caz^2+abw^2, \tag{9}$$

如果

$$f_1=f(x_1,y_1,z_1,w_1)=x_1^2+bcy_1^2+caz_1^2+abw_1^2,$$

则

$$f_2=ff_1=f(x_2,y_2,z_2,w_2),$$

这里

$$x_2=xx_1-(bcyy_1+cazz_1+abww_1),$$
$$y_2=yx_1+xy_1+a(zw_1-wz_1),$$
$$z_2=zx_1+xz_1+b(wy_1-yw_1),$$
$$w_2=wx_1+xw_1+c(yz_1-zy_1)。$$

因此，如果f能表示m和n，则f也能表示mn。

定理 7 如果同余式

$$cX^2+bY^2+a\equiv 0(\bmod n)$$

对于X，Y有解，则方程

$$f(x,y,z,w)=mn,\ |m|\leqslant\sqrt{2|abc|}$$

有一组不全为零的整数解。

作为(9)的一个特殊情形($a=b=c=1$)，Lagrange早已证明：任一正整数都可表为四个数的平方和，即有

定理 8 对任一正整数n，方程

$$x^2+y^2+z^2+w^2=n$$

都有整数解x,y,z和w。

§7 一些与二次丢番图方程有关的问题和结果

关于二次丢番图方程有一些有趣的问题和结果，有些问题直到现在也没有得到解决。

Ⅰ. Ankeny，Artin和Chowla 曾经提出如下的猜想：设$p\equiv 1 \pmod 4$是一个素数，且有整数x，y使

$$x^2-py^2=-4。$$

如果Y是y的最小正值，则$Y\not\equiv 0 \pmod p$。

Goldberg证明了猜想在$p<2000$，且$p\equiv 5 \pmod 8$或$p<100000$，$p\equiv 1 \pmod 8$时是正确的。Mordell[21]和Chowla分别证明了当$p\equiv 5 \pmod 8$和$p\equiv 1 \pmod 8$时，$Y\not\equiv 0 \pmod p$的充要条件是

$$B_{\frac{p-1}{4}}\not\equiv 0 \pmod p,$$

这里B_n是Bernouilli数，由下式定义

$$\frac{t}{e^t-1}=1-\frac{t}{2}+\sum_{n=1}^{\infty}(-1)^{n+1}\frac{B_n t^{2n}}{(2n)!}。\qquad (1)$$

由Bernouilli数与丢番图方程的特殊关系(Bernouilli数与Fermat大定理关系最为密切)，故它引起了许多人的关注。

我们定义序列b_n如下

$$b_0=1,\quad (m+1)b_m=-\sum_{k=0}^{m-1}\binom{m+1}{k}b_k\ (m\geq 1), \tag{2}$$

则有

定理 1 对所有$n\geq 1$，均有$b_{2k+1}=0$和$b_{2n}=(-1)^{n+1}$。B_n。

证 由于$\frac{t}{e^t-1}$展成幂级数为

$$\frac{t}{e^t-1}=\sum_{m=0}^{\infty}\frac{b'_m t^m}{m!}, \tag{3}$$

故

$$t=\sum_{n=1}^{\infty}\frac{t^n}{n!}\sum_{m=0}^{\infty}b'_m\frac{t^m}{m!},$$

比较t^{m+1}的系数给出$b'_0=1$（对$m=0$）和

$$\sum_{k=0}^{m}\binom{m+1}{k}b'_k=0。$$

由此即推出$b'_m=b_m(m\geq 0)$。又由(2)知$b_1=-\frac{1}{2}$，$b_{2n+1}=0$ $(n\geq 1)$，故(3)式即为

$$\frac{t}{e^t-1}=1-\frac{t}{2}+\sum_{n=1}^{\infty}\frac{b_{2n}t^{2n}}{(2n)!},$$

由此与(1)比较得$b_{2n}=(-1)^{n+1}B_n$。证毕。

利用(2)式的递推关系，很容易给出前面一些Bernouilli数B_n。例如由(2)式得

$$1+2b_1=0$$

$$1+3b_1+3b_2=0$$

$$1+4b_1+6b_2+4b_3=0$$

$$1+5b_1+10b_2+10b_3+5b_4=0$$

……

由此解出$b_1=-\frac{1}{2}$，$b_2=\frac{1}{6}$，$b_4=-\frac{1}{30}$，$b_3=\frac{1}{42}$，…，故B_n $(n\geqslant 1)$有如下的序列

$$\frac{1}{6},\ \frac{1}{30},\ \frac{1}{42},\ \cdots。$$

注意：$B_n\equiv a(\bmod p)$定义为：设$B_n=\frac{U_n}{V_n}$，则$V_n^{-1}U_n\equiv a(\bmod p)$。关于Bernouilli数在第八章中还将用到。

另一个猜想是：设$p\equiv 3(\bmod 4)$是素数，且有

$$x^2-py^2=1,\ x,y\in Z。$$

如果$\overline{Y}$是y的最小正值，则$\overline{Y}\not\equiv 0(\bmod p)$。

Goldberg证明了$p<18000$时猜想是正确的，Mordell[22]证明了$\overline{Y}\not\equiv 0(\bmod p)$的充要条件是

$$E_{\frac{p-3}{4}}\not\equiv 0(\bmod p),$$

这里E_n是Euler数，由下式定义

$$\operatorname{Sec}t=\sum_{n=0}^{\infty}\frac{E_n t^{2n}}{(2n)!}。$$

Ⅱ．Grescenzo[23]在1975年提出了如下问题：是否存在无穷多对素数p,q适合

$$p^2-2q^2=-1? \tag{4}$$

类似地，我们可以提出如下问题：是否存在无穷多对素数p,q适合

$$p^2-5q^2=-4? \tag{5}$$

这是两个没有解决的问题。1986年，屈明华[24]对方程(4)证明了：

在$p,q<10^{15}$时，仅有三对素数p,q适合(4)，即$(p,q)=$

(7, 5), (41, 29)和(63018038201, 44560482149)。同时，他还证明了如下的几个结果：

定理 2 设$q\equiv 1(\mathrm{mod}\,8)$是素数，如果$q=u^2+2v^2$，$8\nmid v$，则对任意素数$p$，(4)不成立。

定理 3 如果$p=u^2+2v^2\equiv 9(\mathrm{mod}\,16)$是素数，$8|v$，则对任意素数$q$，(4)不成立；如果$p=c^2+128d^2\equiv 17(\mathrm{mod}\,32)$是素数，这时$p$也可表成$p=a^2+64b^2$，则在$b+d\equiv 1(\mathrm{mod}\,2)$时，对任意素数$q$，(4)式均不成立。

定理 4 设$f\equiv -1(\mathrm{mod}\,4)$，$f>11$是素数。如果

1) $p=2f+1$ 是素数，则对任意素数 q，(4)不成立，

2) $q=2f-1$ 是素数，则对任意素数 p，(4)不成立。

定理 5 设$f\equiv 1(\mathrm{mod}\,4)$，$f>11$是素数。如果

1) $q=6f-1$ 是素数，则对任意素数 p，(4)不成立。

2) $p=6f+1$ 是素数，则对任意素数 q，(4)不成立。

对于方程 (5)，目前还没有什么工作，估计是很难回答的。但对于方程$p^2-2q^2=1$和$p^2-5q^2=4$（这里p,q均为素数)却十分容易。例如取模3即可分别得出仅有唯一解$(p,q)=(3,2)$和$(p,q)=(7,3)$。Cassels[25]曾得出了一个有趣的定理。

定理 6 设P是素数的一个有限集，Π是素因子$\in P$的全体正整数的集。再设$F>0$，$E\neq 0$是整数，且E的素因子$\notin P$，则二次丢番图方程

$$X^2-FY^2=E,\quad X\in Z,\quad Y\in \Pi$$

仅有有限组解X，Y。

这个定理在证明高次丢番图方程仅有有限个解时，也是一个得力的工具。

参 考 文 献

[1] Lienen, V.H., J.Number Theory,10(1978), 10—15.

[2] Golomb,S.W., Amer. Math. Monthly, 77(1970), 848—852.

[3] Makowski, A., Amer. Math.Monthly, 79(1972), 761.

[4] Sentance, W.A., Amer. Math. Monthly, 88(1981), 272—274.

[5] 肖戎，数学研究与评论，3(1987)，408—410.

[6] 袁平之,关于 Golomb 猜想（已投《数学研究与评论》）。

[7] Ljunggren, W.,Norsk Mat. Tidsskr., 23(1941), 132—138.

[8] Baker, A. and Davenport, H.,Quart.J. Math. Oxford, 20(1969), 129—137.

[9] Kanagasabapathy, P.and Ponnudurai, T., Quart.J. Math. Oxford, 26(1975), 275—278.

[10] Veluppillai, M., The Fibonacci sequence, Collect. Manuscr., 18th anniv.Vol., The Fibonacci Assoc., 1980, 71—75.

[11] 曹珍富，数学杂志，3(1983)，227—235.

[12] Mohanty, S.P. and Ramasamy,A.M.S., J. Number Theory, 18(1984), 356—359.

[13] 曹珍富，科学通报，6(1986)，476.

[14] 曹珍富，孙显奕,太原机械学院学报，1986，No.2.

[15] Ljunggren, W., Norsk Mat. Tidsskr., 26(1944), 3—8.
[16] Ljunggren, W., Norsk Vid. Selsk. Forh., Trondhjem, 15(1942), 67—70.
[17] Trost, E., Vierteljsehr. Naturforsch. Ges. Zürich 85 Beiblatt(Festschrift Rudolf Fueter), 1940, 138—142.
[18] 柯召、孙琦，谈谈不定方程，上海教育出版社(1980)，41—44.
[19] Ryser, H. J., Combinatorial Mathematics, 1963。中译本：组合数学（李乔译），科学出版社（1983），85页。
[20] 柯召，四川大学学报（自然科学版），6 (1959), 1—10.
[21] Mordell, L.J., Acta Arith., 6(1960), 137—144.
[22] Mordell, L.J., J. London Math. Soc., 36(1961), 282—288.
[23] Grescenzo, P., Advance Math., 17(1975), 25—29.
[24] 屈明华，四川大学学报（自然科学版），2(1986), 1—9.
[25] Cassels, J.W.S., Ark.Mat.,4(1961), 231—233.
[26] 裴定一，科学通报，24(1982), 1476—1478.

第六章　三次丢番图方程

解三次丢番图方程是一个十分困难的问题，即使对于方程 $y^2=x^3+k$（k 给定）也是如此。然而，在丢番图分析，代数数论和编码理论等领域中要用到不少类型的三次丢番图方程的结果，这就迫使我们来研究三次丢番图方程的一些基本类型的解法。

§1　方程$ey^2=ax^3+bx^2+cx+d$，$a\neq 0$

给定整数a，b，c，d 和e（这里$a\neq 0$），我们来研究方程

$$ey^2=ax^3+bx^2+cx+d \tag{1}$$

的整数解。以$81e$乘（1）的两端，记 $y_1=9ey$，$x_1=3x$，则（1）化为。

$$y_1^2=(3ae)x_1^3+(9be)x_1^2+(27ce)x_1+(81de)。$$

令$t=6aey_1$，$s=3aex_1+3be$，则上式又化为

$$t^2=g_1s^3-g_2s-g_3, \tag{2}$$

其中$g_1=4$，$g_2=108e^2(b^2-3ac)$和$g_3=108e^3(b^3-27a^2d-3b)$。在（2）的两端同乘$g_1^2$得

$$u^2=v^3-\lambda v-\eta, \tag{3}$$

这里$u=g_1t$，$v=g_1s$是变元，$\lambda=g_1g_2$和$\eta=g_1^2g_3$ 是给定的。这样，以下不失一般可仅讨论方程（3）的解，且设 λ，

η 不能同时为零。

Ⅰ．先看 $\lambda=0$。此时（3）化为著名的Mordell方程

$$u^2=v^3-\eta,\ \eta\neq 0。\tag{4}$$

Baker[1] 用他的有效方法证明了方程（4）的所有整数解u，v均满足

$$\max(|u|,|v|)<\exp(10^{10}|\eta|^{10^4}),$$

这里$\exp(*)=e^*$。后来，Stark在1973年又改进了Baker的结果，得到

定理 1 方程（4）的所有整数解u，v均满足

$$\max(|u|,|v|)<\exp(c|\eta|^{1+\varepsilon}),$$

这里对$\forall\varepsilon>0$，$c=c(\varepsilon)$是可以有效确定的。

这个定理虽然给出了方程（4）解的绝对值上界，但对给定η给出方程（4）的全部解仍有困难。正因为如此，对具体η给出方程（4）的全部解就成为一件重要的事情。

利用简单同余法，可以得到方程(4)无解的一些简单结果，例如，设

1） $\eta=4a^2-(4b-1)^3$，a不含$4k+3$形的素因子，或

2） $\eta=(2a+1)^2-(4b+2)^3$，$2a+1$不含$4k+3$形的素因子，或

3） $\eta=a^3+2b^2$，$a\equiv 4$，$6(\mathrm{mod}\,8)$，$b\equiv 1(\mathrm{mod}\,2)$且$b$不含$8k+5$和$8k+7$形的素因子，或

4） $\eta=a^3-2b^2$，$a\equiv 2$，$4(\mathrm{mod}\,8)$，$b\equiv 1(\mathrm{mod}\,2)$且$b$不含$8k\pm 3$形的素因子，或

5） $\eta=a^3-3b^2$，$a\equiv 1(\mathrm{mod}\,4)$，$b\equiv\pm 2(\mathrm{mod}\,6)$且$b$不含$12k\pm 5$形的素因子。则方程（4）均无整数解。

现在给出在3)和5)时方程(4)无整数解的证明(其余类似可证)。在3)时，由假设知$\eta\equiv 2(\mathrm{mod}\,8)$。因此如果(4)有解，则

给出 $2\nmid uv$。于是对（4）取模 8 得 $1\equiv v-2(\bmod 8)$，即$v\equiv 3(\bmod 8)$，这样就有$v-a\equiv 7, 5(\bmod 8)$。于是对方程（4）取模$v-a$得（注意$\eta=a^3+2b^2$）

$$u^2\equiv -2b^2(\bmod v-a)。\qquad (5)$$

由于$v-a\equiv 5, 7(\bmod 8)$，故必有素数$p\equiv 5, 7(\bmod 8)$使得$p\mid v-a$。由b不含$8k+5$或$8k+7$形素因子知，$p\nmid b$。于是（5）给出

$$1=\left(\frac{-2b^2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=-1,$$

这不可能。

在 5）时，由于 $\eta=a^3-3b^2\equiv a(\bmod 3)$，故（4）给出$v\equiv a, a+1(\bmod 3)$。

如果$v\equiv a(\bmod 3)$，则$v^3\equiv a^3(\bmod 9)$，（4）推出 $u^2\equiv 3b^2\equiv 3(\bmod 9)$，此不可能。如果$v\equiv a+1(\bmod 3)$，则$v^2+av+a^2\equiv 1(\bmod 3)$。又由 $\eta=a^3-3b^2\equiv 1(\bmod 4)$ 知，（4）给出$v\equiv 1(\bmod 4)$，故$v^2+av+a^2\equiv 3(\bmod 4)$。从而 $v^2+av+a^2\equiv 7(\bmod 12)$。故对（4）取模$v^2+av+a^2$得

$$u^2=3b^2+v^3-a^3\equiv 3b^2(\bmod v^2+av+a^2)。\qquad (6)$$

由$v^2+av+a^2\equiv 7(\bmod 12)$知，必有素数 $p\equiv \pm 5(\bmod 12)$满足$p\mid v^2+av+a^2$，且由b不含$12k\pm 5$形的素因子知 $p\nmid b$。于是（6）式给出$1=\left(\frac{3b^2}{p}\right)=\left(\frac{3}{p}\right)=-1$，这也不可能。

按照以上思路，可以用简单同余法证明较为一般的结论。例如对$\eta=a^3-kb^2$，方程（4）化为

$$u^2-kb^2=v^3-a^3。\qquad (7)$$

通过对a，b和k的一些假设条件，使得$v-a$ 或v^2+av+a^2含

有某奇素因子 p，$p \nmid b$，$\left(\frac{k}{p}\right)=-1$，则对这些假设条件而言，（7）无整数解。Mordell [2] 证明了

定理 2 设 $\eta=k^3a^3-kb^2$，这里 a,b,k 满足以下三个条件：

1） $a\equiv 3(\bmod 4)$，$b\equiv 0(\bmod 2)$；

2） $k\equiv 3(\bmod 4)$ 无平方因子，$(k, b)=1$，且当 $k\equiv 2(\bmod 3)$ 时 $b\not\equiv 0(\bmod 3)$；

3） a和b没有共同的素因子p 满足$\left(\frac{k}{p}\right)=-1$，则方程（4）无整数解$u$，$v$。

有些形如（4）的方程是有整数解的。例如早在1621年，Bachet就发现方程$u^2=v^3-2$有整数解$u=\pm 5$，$v=3$。Fermat曾要求证明这也是仅有的整数解。后来，Euler给出了一个错误的证明（参阅[3]）。下面我们将看到，Fermat要求证明的结论利用代数数论方法能够十分容易地证明，而且更一般地有

定理 3 设$\eta>1$无平方因子，$\eta\equiv 2$或$1(\bmod 4)$。如果二次域$Q(\sqrt{-\eta})$的类数不被3整除，则方程（4）有整数解的充分必要条件是η具有$3t^2\pm 1$的形状。并且如果 $\eta=3t^2\pm 1$，则（4）仅有解为$u=\pm t(t^2-3\eta)$，$v=t^2+\eta$。

证 显然，$\eta=3t^2\pm 1$时，（4）有解 $u=\pm t(t^2-3\eta)$，$v=t^2+\eta$。下面我们证明如果方程（4）有解，则η具有$3t^2\pm 1$的形状，且当 $\eta=3t^2\pm 1$ 时（4）仅有解 $v=t^2+\eta$，$u=\pm t(t^2-3\eta)$。为此，我们在二次域$Q(\sqrt{-\eta})$中来考虑方程（4）。

如果方程（4）有解，则 $v\equiv 1(\bmod 2)$且$(v, \eta)=1$。由

(4) 得理想数方程

$$[u+\sqrt{-\eta}][u-\sqrt{-\eta}]=[v]^3。\qquad(8)$$

由于$\eta\equiv2$或$1(\bmod 4)$，故$-\eta\equiv2,3(\bmod 4)$，因此$Q(\sqrt{-\eta})$中的整数为$t+s\sqrt{-\eta}$ (t, $s\in Z$)，单位数为±1。现在证明$([u+\sqrt{-\eta}],[u-\sqrt{-\eta}])=[1]$。不然若有素理想$P|([u+\sqrt{-\eta}],[u-\sqrt{-\eta}])$，则$P|2\sqrt{-\eta}$，$P|v$。因此$N(P)|4\eta$，且$N(P)|v^2$，而这不可能。故由（8）给出

$$[u+\sqrt{-\eta}]=A^3,\qquad(9)$$

这里A是$Q(\sqrt{-\eta})$的某些理想数。因为二次域$Q(\sqrt{-\eta})$的类数不被3整除，因此A是一主理想数，故（9）式给出

$$u+\sqrt{-\eta}=\pm(t+s\sqrt{-\eta})^3,$$

$$v=N(A)=t^2+\eta s^2。$$

由此得出

$$1=\pm s(3t^2-\eta s^2),\quad u=\pm t(t^2-3\eta s^2),\quad v=t^2+\eta s^2,$$

故由第一式给出$s=\pm1$，因此$\eta=3t^2\pm1$，$u=\pm t(t^2-3\eta)$，$v=t^2+\eta$。证毕。

在定理3中取$\eta=2$，13时，由于$h(-2)=1$，$h(-13)=2$，故得

推论 方程$u^2=v^3-2$仅有整数解$u=\pm5$，$v=3$；方程$u^2=v^3-13$仅有整数解$u=\pm70$，$v=17$。

定理 4 设$-\eta>1$，η无平方因子，$\eta\equiv2$或$1(\bmod 4)$，二次域$Q(\sqrt{-\eta})$的类数不被3除尽。再设$x^2+\eta y^2=1$的基本解为$\varepsilon=x_0+y_0\sqrt{-\eta}$，则方程（4）有整数解推出

$$x_0(3a^2b-\eta b^3)\pm y_0(a^3-3\eta ab^2)=1,\qquad(10)$$

这里a，b是某些整数。

证 改写方程（4）为$Q(\sqrt{-\eta})$中理想数方程

$$[u+\sqrt{-\eta}][u-\sqrt{-\eta}]=[v]^3。$$

由定理3的证明可得

$$[u+\sqrt{-\eta}]=A^3,$$

由于 $Q(\sqrt{-\eta})$ 的类数不被3除尽，故上式给出 A 是一个主理想，于是知

$$u+\sqrt{-\eta}=\rho^n(t+s\sqrt{-\eta})^3,\ n=0,\ \pm 1, \quad (11)$$

$$v=t^2+\eta s^2,$$

其中 ρ 是 $Q(\sqrt{-\eta})$ 中的基本单位数。这里不妨取 $\rho=\varepsilon=x_0+y_0\sqrt{-\eta}$，因为如果 $N(\rho)=-1$，则 $\rho^2=\varepsilon, \rho=\dfrac{\rho^3}{\varepsilon}$，而 ρ^3 可以并入括号，于是（11）给出

$$u+\sqrt{-\eta}=\varepsilon^n(t+s\sqrt{-\eta})^3,\ n=0,\ \pm 1。\quad (12)$$

当 $n=0$ 时，（12）给出 $\eta=3t^2\pm 1$，但 $-\eta>1$，故不可能。而 $n=\pm 1$ 时，（12）给出（10）式。证毕。

推论 1 设 $\eta<0$，$Q(\sqrt{-\eta})$ 的类数不被3除尽 $\eta\equiv 2$ 或 $1(\mathrm{mod}4)$。且设 $x^2+\eta y^2=1$ 的基本解为 $\varepsilon=x_0+y_0\sqrt{-\eta}$。则当 $\eta\equiv -4\ (\mathrm{mod}9)$，$y_0\equiv 0(\mathrm{mod}9)$ 或 $\eta\equiv 2(\mathrm{mod}9)$，$y_0\equiv \pm 3(\mathrm{mod}9)$ 时，方程（4）无整数解。

证 由定理4利用简单同余法即得。

由推论可推出当 $\eta=-7,\ -34,\ -58,\ -70$ 等时方程（4）均无整数解。

现在我们考虑二次域 $Q(\sqrt{-\eta})$ 的类数 $h(-\eta)\equiv 0(\mathrm{mod}3)$ 的情形。设 $\eta\equiv 2$ 或 $1(\mathrm{mod}4)$，η 无平方因子，且 $h(-\eta)\equiv 0(\mathrm{mod}3)$。由定理3的证明知 $(u+\sqrt{-\eta}, u-\sqrt{-\eta})=1$，故（4）给出

$$[u+\sqrt{-\eta}]=A^3,\ [u-\sqrt{-\eta}]=B^3,\ [v]=AB。$$

设 C 是 A 的逆类中的理想（即 $AC=[a+b\sqrt{-\eta}]$ 为主理想

数），则

$$C^3[u+\sqrt{-\eta}]=(AC)^3=[a+b\sqrt{-\eta}]^3,$$

这里a，b是有理整数。由此可知

$$C^3=[p+q\sqrt{-\eta}],\ p^2+\eta q^2=N(C)^3=n^3,$$

这里p，q是有理整数。于是有理想数方程

$$n^3[u+\sqrt{-\eta}]=\rho[p-q\sqrt{-\eta}][a+b\sqrt{-\eta}]^3, \tag{13}$$

这里ρ是$Q(\sqrt{-\eta})$中的单位。如果$\eta>0$，则ρ可取1；如果$\eta<0$，则$\rho=1$，ε，ε^{-1}，这里$\varepsilon=x_0+y_0\sqrt{-\eta}$是Pell方程$x^2+\eta y^2=1$的基本解。至于$n$的取值，当C是一个主理想数时，可取$n=1$；当C是一个素理想数时，$n$将是一个素数。于是，方程（13）可化为关于$X$，$Y$的三次方程

$$a_1X^3+3a_2X^2Y+3a_3XY^2+a_4Y^3=a_5^3。\tag{14}$$

利用简单同余法可证明在某些条件下，方程(14)无整数解。

对于$\eta>0$，$\eta\equiv-1(\bmod 8)$，$\eta\neq7$和$h(-\eta)=3$的情形，我们有

定理 5 设$\eta>0$，$\eta\equiv-1(\bmod 8)$，$\eta\neq7$且η无平方因子。再设$h(-\eta)=3$，则方程（4）无$2|v$的整数解。

证 在$\eta>0$，$\eta\equiv-1(\bmod 8)$时，$Q(\sqrt{-\eta})$的整底是1，ω（这里$\omega=\dfrac{1+\sqrt{-\eta}}{2}$）。我们有2的理想数分解为

$$[2]=[2,\ 1+\omega][2,1+\omega']=AB,$$

这里ω'是ω的共轭。由于对整数a，b有

$$2\nmid(a+b\omega)(a+b\omega'),$$

（这是因为$2=(a+b\omega)(a+b\omega')$推出$8=(2a+b)^2+\eta b^2$，而$\eta\neq7$，故$8\neq(2a+b)^2+\eta b^2$），故$A$，$B$均不是主理想数。如果方程（4）有$2|v$的整数解，则由$A\neq B$知$(u+\sqrt{-\eta}, u-\sqrt{-\eta})=2$。于是由方程（4）给出

$$[u+\sqrt{-\eta}]=[2]AD^3,$$

因为 D^3 是主理想数，而 A 不是主理想数，故上式不成立。证毕。

推论 2 设 $\eta=a^2+b^3>0$，$b\not\equiv 1(\bmod 4)$，a 无 $4k+3$ 形的素因子。且设 $\eta\equiv -1(\bmod 8)$，η 无平方因子和 $h(-\eta)=3$，则方程（4）无整数解。

证 由定理 5 知，只要证明方程（4）无 $2\nmid v$ 的整数解。在 $2\nmid v$ 时，由于 $\eta\equiv -1(\bmod 8)$，所以 $v\equiv 3(\bmod 4)$。现把(4)改写为

$$u^2+a^2=v^3-b^3=(v-b)(v^2+vb+b^2), \tag{15}$$

由于 $b\equiv 2$，$3(\bmod 4)$ 时，$v^2+vb+b^2\equiv 3(\bmod 4)$；$b\equiv 0(\bmod 4)$ 时，$v-b\equiv 3(\bmod 4)$。故在 $b\not\equiv 1(\bmod 4)$ 时，(15) 式不成立。证毕。

利用三次剩余特征也可以研究方程（4）的无解性。例如利用 $\left(\frac{2}{p}\right)_3=1\Longleftrightarrow p=r^2+27s^2$；$\left(\frac{3}{p}\right)_3=1\Longleftrightarrow 4p=r^2+243s^2$，Hall[4] 证明了

定理 6 设 $\eta=-2a^3+3b^2$，$ab\neq 0$，$a\not\equiv 1(\bmod 3)$，$b\not\equiv 0(\bmod 3)$，且当 $b\equiv 0(\bmod 2)$ 时，$a\equiv 1(\bmod 2)$。如果 2 是奇素数 $p\equiv 1(\bmod 3)$ 的三次剩余，$p\mid a$，则方程(4)无整数解。

定理 7 设 $\eta=-4a^3+3b^2$，$ab\neq 0$，$a\equiv 0$，$2(\bmod 6)$，$b\equiv \pm 1(\bmod 6)$，且 a 没有 $3k+1$ 形的素因子。则方程（4）没有整数解。

定理 8 设 $\eta=-3a^3+3b^2$，$a^3-b^2\not\equiv 0(\bmod 3)$，且 b，$b\pm(1+\eta)$ 中的每一个均不被3整除，或被 3 整除但不被 9 整除，则方程（4）无整数解。

还有一些形如（4）的丢番图方程，解决起来是很难的。例如，下面两个定理的证明都用到Baker 的有效方法，且计算也较为复杂。

定理 9[5] 丢番图方程$y^2+28=x^3$仅有整数解$(x,y)=(4,\ \pm 6)$，(8 ± 22)和$(37,\ \pm 225)$。

定理10[6] 丢番图方程 $y^2+999=x^3$ 仅有正整数解 $(x,y)=(10,\pm 1),(12,\pm 27),(40,\pm 251),(147,\pm 1782),(174,\pm 2295)$和$(22480,\pm 3370501)$。

定理10完整地回答了 Stolarsky[7] 的一个问题。下面我们来证明，除$x=147$，$y=\pm 1782$外，方程 $y^2+999=x^3$可化为

$$X^3-4XY^2+2Y^3=1, \tag{16}$$

为此我们要用到Hemer[8]的一个结果。

定理11 设$K=kf^2$，k无平方因子，且$(f,\ x^3)$无三次方因子。如果$2f$含有r个不同素因子 $p_i(i=1,\ \cdots,\ r)$，在$Q(\sqrt{k})$中$p_i=P_iP_i'$，且$Q(\sqrt{k})$的类数$h(k)\neq 0(\mathrm{mod}\,3)$，则方程$y^2-kf^2=x^3$的所有整数解可由下式得到：

$$\prod_{i=1}^{r} p_i^{q_i}(\pm y+f\sqrt{k})=\prod_{i=1}^{r} P_i^{h_i}A^3=\rho BA^3,$$

这里$h_i=0$或使$P_i^{h_i}$是一个主理想数的最小正整数，且考虑所有这些值的组合。当$h_i=0$时，我们令 $q_i=0$；当 $h_i>0$（因此$h\neq 0(\mathrm{mod}\,3)$）时，如果$h_i\equiv 1(\mathrm{mod}\,3)$，则令$q_i=h_i-2$，且如果$h_i\equiv 2(\mathrm{mod}\,3)$，则$q_i=h_i-1$。这里$A$是$Q(\sqrt{k})$中的整数。如果$k>0$，则$\rho=1,\varepsilon,\varepsilon^{-1}$，这里$\varepsilon$是 $Q(\sqrt{k})$的基本单位。如果$k<0$且$k\neq 3$，则 $\rho=1$，而$k=3$，则 $\rho=1$或$\dfrac{1+\sqrt{-3}}{2}$。

现在，对方程$y^2+999=x^3$，有$K=-999=-111\cdot 3^2$，

故$f=3$，$k=-111$。因为$-111\equiv1(\mathrm{mod}8)$，在$Q(\sqrt{-111})$中有$[2]=P_2P_2'$。由于$Q(\sqrt{-111})$的类数$h(-111)=8$，且

$$2^8=\left(\frac{5+3\sqrt{-111}}{2}\right)\left(\frac{5-3\sqrt{-111}}{2}\right)$$

是2分解为两个主理想乘积的最小幂。因此，由定理11知，方程$y^2+999=x^3$给出如下的两种情形：

$$\pm y+3\sqrt{-111}=\left(\frac{a+b\sqrt{-111}}{2}\right)^3, \qquad (17)$$

$$128(y+3\sqrt{-111})=\left(\frac{5+3\sqrt{-111}}{2}\right)\left(\frac{a+b\sqrt{-111}}{2}\right)^3。 \qquad (18)$$

在（17）时，给出

$$a^2b-37b^3=8，推出a=12，b=-2，$$

故给出$x=147$，$y=\pm1782$。而（18）式推出

$$a^3+5a^2b-333ab^2-185b^3=2048。$$

令$a=X+Y$，$b=Y$，则

$$X^3+8X^2Y-320XY^2-512Y^3=2048。$$

由此知$X\equiv0(\mathrm{mod}8)$。X用$8X$换，则有

$$X^3+X^2Y-5XY^2-Y^3=4，$$

X用$X+Y$换，Y用X换，则上式给出

$$\pm4X^3+4XY^2+Y^3=4。$$

由此推出$Y\equiv0(\mathrm{mod}2)$。故用$-X$换X，$2Y$换Y，上式即为（16）。Steiner 用了十分冗长且不是初等的方法证明了（16）式仅有整数解$(X,Y)=(-1,-1)$，$(1,0)$，$(1,1)$，$(-5,-3)$和$(-31,14)$。在第三章§4的习题中，我们给出了用p-adic方法证明的提示。此外，Ljunggren[9] 还证

明了方程$y^2+7=x^3$仅有整数解$(x,y)=(2,\pm1)$和$(32,\pm181)$；方程$y^2-15=x^3$仅有整数解$(x,y)=(1,\pm4)$。Nagell[10] 证明了$y^2=x^3+17$有8个整数解$(x,y)=(-1,4),(-2,3),(2,5),(4,9),(8,23),(43,282),(52,375)$和$(5234,378661)$。London和Finkelstein[11] 完全解决了$\eta=18, 25, 100$的情形。这样由定理9便知$|\eta|\leqslant100$全部得到解决[9]，还有一些结果见[12]。

Ⅱ. 现在设（3）中$\lambda\neq0$

定理12 设（3）式右端不可能分解为$(Au+B)^2(Cu+D)$的形状，则方程（3）最多只有有限个解。

但是，要求出（3）的全部解来，即使对于给定系数的情形也是十分困难的。例如，Lucas曾经问：方程

$$6y^2=x(x+1)(2x+1) \tag{19}$$

是否仅有整数解$(x,y)=(0,0), (-1,0), (1,\pm1), (24,\pm70)$？过了很长时间才由Watson[13] 在1919年利用椭圆函数给出了肯定的回答。1952年，Ljunggren[14] 利用四次扩域中的Pell方程又给出了一个证明。Mordell 问：能否给出一个初等的证明？1985年，马德刚[15]，徐肇玉和曹珍富[16]分别独立地解决了这个问题，他们用初等的方法证明了

定理13 丢番图方程（19）仅有整数解$(x,y)=(0,0), (-1,0), (1,\pm1)$和$(24,\pm70)$。

证 除开$(x,y)=(0,0), (-1,0)$外，只要证明方程（19）仅有正整数解$(x,y)=(1,1)$和$(24,70)$。由于$(x(x+1), 2x+1)=1$，故（19）给出

$$x(x+1)=2y_1^2,\quad 2x+1=3y_2^2,\quad y=y_1y_2, \tag{20}$$

或

$$x(x+1)=6y_1^2,\quad 2x+1=y_2^2,\quad y=y_1y_2。 \tag{21}$$

由（21）给出 $y_2^4-6(2y_1)^2=1$，熟知，此方程仅有正整数解 $y_1=10$，$y_2=7$（参阅第七章），故给出方程（19）的正整数解 $x=24$，$y=70$。现在我们用递推序列方法证明（20）仅有正整数解 $x=1$，$y=1$。由(20)的第二式显然 $x\neq 2y_3^2$，于是（20）给出

$$x=y_3^2,\quad x+1=2y_4^2,\quad 2x+1=3y_2^2,$$

而这些方程给出丢番图方程组

$$\begin{aligned}2y_3^2-3y_2^2&=-1,\\4y_4^2-3y_2^2&=1。\end{aligned}\qquad(22)$$

由（22）的第二个方程可得

$$(6y_2^2+1)^2-3(4y_2y_4)^2=1,$$

利用Pell方程的解法（参见第五章），有

$$6y_2^2+1+4y_2y_4\sqrt{3}=(2+\sqrt{3})^n,\quad n\geqslant 0。\qquad(23)$$

令 $U_n+V_n\sqrt{3}=(2+\sqrt{3})^n$，$\varepsilon=2+\sqrt{3}$，$\bar{\varepsilon}=2-\sqrt{3}$，则（23）给出

$$6y_2^2+1=U_n=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2},\quad n\geqslant 0。$$

于是由（22）的第一个方程得 $4y_3^2=6y_2^2-2=U_n-3$，即

$$4y_3^2=U_n-3。\qquad(24)$$

下面通过对 U_n，V_n 的一些性质的讨论，证明（24）仅有解 $y_3^2=1$。首先直接验证可有如下的关系

$$\begin{aligned}U_{n+m}&=U_nU_m+3V_nV_m,\\V_{n+m}&=U_mV_n+V_mU_n,\\U_{-n}&=U_n,\quad V_{-n}=-V_n,\\U_{2n}&=U_n^2+3V_n^2=2U_n^2-1\\&=6V_n^2+1,\quad V_{2n}=2U_nV_n,\end{aligned}$$

由此可推出

$$U_{n+2t} \equiv U_n(\bmod V_r),\quad U_{n+2r} \equiv -U_n(\bmod U_r),$$

进而有

$$U_{n+2rt} \equiv U_n(\bmod V_r),\quad U_{n+2rt} \equiv (-1)^t U_n(\bmod U_r)。\tag{25}$$

由$\varepsilon=2+\sqrt{3}$可得递推序列

$$U_{n+2}=4U_{n+1}-U_n,\quad V_{n+2}=4V_{n+1}-V_n,\tag{26}$$

且经简单计算有下表：

表 1

n	0	1	2	3	4	5	6	10
U_n	1	2	7	26	97	362	1351	262087
V_n	0	1	4	15	56	209	780	151316
$U_n(\bmod 5)$	1	2	2	1	2	2	1	2
$U_n(\bmod 8)$	1	2	-1	2	1	2	-1	
$U_n(\bmod 3)$	1	-1	1	-1	1	-1	1	
$V_n(\bmod 8)$	0	1	4	-1	0	1	4	

现在，我们分6种情况来讨论：

(a) 若 $n\equiv1(\bmod 2)$，则（24）不成立。这是因为在$n\equiv1(\bmod 2)$ 时 $U_n\equiv0(\bmod 2)$。

(b) 若 $n\equiv 0(\bmod 20)$，则（24）不成立。$n=0$ 时（24）显然不成立。设 $n\neq0$，$n=2\cdot5\cdot2^t k$，$t\geqslant1$，$2\nmid k$，则由（25）式知$U_n\equiv U_0(\bmod U_5)$。故若（24）成立推出

$$4y_3^2\equiv U_0-3\equiv-2(\bmod U_5),$$

但 $181\mid U_5$，$181\equiv5(\bmod 8)$，因此上式给出 $1=\left(\frac{-2}{181}\right)=\left(\frac{2}{181}\right)=-1$ 的矛盾结果。

(c) 若$n\equiv\pm2(\bmod 20)$，$n\neq2$，则（24）不成立。不然，可写$n=\pm2+20s=\pm2+2\cdot k\cdot 5l$，这里$k=2^t$，$t\geqslant1$，$2\nmid l$。于是（25）给出$U_n\equiv-U_{\pm2}(\bmod U_k)$，（24）给出

$$4y_3^2\equiv-U_{\pm2}-3\equiv-10(\bmod U_k)。\qquad(27)$$

如果$t>1$，则$k=2^t\equiv0(\bmod 4)$。由表1及（26）式知$U_k\equiv1(\bmod 8)$，故由（27）并注意表1知

$$1=\left(\frac{-10}{U_k}\right)=\left(\frac{5}{U_k}\right)=\left(\frac{U_k}{5}\right)=-1,$$

这不可能。

如果$t=1$，则$n=\pm2+2\cdot10\cdot l$，$2\nmid l$。先看$n=2+2\cdot10\cdot l$，此时$U_n=6V_{1+10l}^2+1\equiv1(\bmod V_{1+10l})$，而$1+10l\equiv3(\bmod 4)$，由表1及（26）式知$V_{1+10l}\equiv-1(\bmod 8)$。直接对（24）取模$V_{1+10l}$得

$$4y_3^2\equiv1-3=-2(\bmod V_{1+10l}),$$

此给出$1=\left(\frac{-2}{V_{1+10l}}\right)=-1$的矛盾结果。

再看$n=-2+2\cdot10\cdot l$，此时$U_n\equiv-U_2(\bmod U_{2l})$，由$2l\equiv2(\bmod 4)$知$U_{2l}\equiv-1(\bmod 8)$，故（24）给出

$$4y_3^2\equiv-U_2-3=-10(\bmod U_{2l}),$$

故得

$$1=\left(\frac{-10}{U_{2l}}\right)=-\left(\frac{5}{U_{2l}}\right)=-\left(\frac{U_{2l}}{5}\right)。\qquad(28)$$

由表1及（26）式，若$l\equiv0(\bmod 3)$，则$\left(\frac{U_{2l}}{5}\right)=1$，与(28)式矛盾。

若$l\equiv1(\bmod 3)$，则$U_n=U_{-2+2\cdot10l}=U_{3t}$。因为$U_{3t}\equiv1(\bmod 5)$，故对（24）取模5知无解。

若$l\equiv 2\pmod 3$，令$l=3s+2$，则$n=-2+2\cdot 10\cdot(3s+2)=2+4(15s+9)=2+2\cdot k\cdot a$，$2\nmid a$，$k=2^t$。由于$2\nmid l$，故推出$t>1$，因此与（27）式类似讨论知（24）此时不成立。

（d） 若 $n\equiv\pm 4,\ \pm 8\pmod{20}$，则（24）不成立。这是因为$n\equiv 0\pmod 4$时$U_n\equiv 1\pmod 8$，故对（24）取模8知无解。

（e） 若$n\equiv\pm 6\pmod{20}$，则（24）不成立。不然，令$n=\pm 6+20\cdot l$，则有$U_n\equiv\pm U_6\pmod{U_{10}}$，于是（24）式给出

$$4y_3^2\equiv\pm U_6-3=\begin{cases}4\cdot 337\\-2\cdot 677\end{cases}\pmod{U_{10}},$$

但从表1知$U_{10}=262087$，故容易验算$\left(\frac{4\cdot 337}{U_{10}}\right)=\left(\frac{-2\cdot 677}{U_{10}}\right)=-1$。

（f） 若$n\equiv 10\pmod{20}$，则（24）不成立。首先$n=10$不成立，所以设 $n=10+20l=2(5+10l)$，$l\neq 0$。若 $l\equiv 1\pmod 2$，则$5+10l\equiv 3\pmod 4$，故 $V_{5+10l}\equiv -1\pmod 8$。所以（24）给出

$$4y_3^2=(6V_{5+10l}^2+1)-3\equiv -2\pmod{V_{5+10l}},$$

此不可能。

若$l\equiv 0\pmod 2$，设$l=2k$，则 $n=10+40k=2+8(1+5k)=2+2\cdot 2^s\cdot a$，$2\nmid a$，$s\geqslant 2$。于是 $U_n\equiv -U_2\pmod{U_{2^s}}$，（24）式给出

$$4y_3^2\equiv -U_2-3=-10\pmod{U_{2^s}}。$$

但由于$s>1$，故由（27）的处理知，这是不可能的。

由$(a)\sim(f)$知，（24）成立仅当 $n=2$，给出$y_3^2=1$。于是知（22）仅有正整数解$y_2=1$，$y_3=1$，$y_4=1$，给出方

程（19）的正整数解$x=1$，$y=1$。证毕。

1963年，Mordell[17]证明了

定理14 方程

$$y(y+1)=x(x+1)(x+2) \tag{29}$$

仅有整数解 $x=-1$，-2，0，1，5。

由于（29）在分别用x，y代$2x+2$，$2y+1$后，可化为

$$2y^2=x^3-4x+2, \tag{30}$$

故只要证明方程（30）仅有整数解 $x=0$，-2，2，4和12。设θ是满足$\theta^3-4\theta+2=0$ 的实数，在三次域$Q(\theta)$中，我们有：

（a） 整数是$a+b\theta+c\theta^2$，这里a，b，$c\in Z$；

（b） 有两个基本单位数$\varepsilon=\theta-1$，$\eta=2\theta-1$；

（c） 由于$Q(\theta)$的理想类数为 1，故$Q(\theta)$中整数唯一分解定理成立。

注意到$2=\xi\theta^3$，这里ξ是一个单位数且θ是$Q(\theta)$中的素数。于是（30）可化为

$$(x-\theta)(x^2+\theta x+\theta^2-4)=\xi\theta^3y^2。$$

从而

$$x-\theta=\pm\theta(4\theta-3)^n\varepsilon^l\eta^m(a+b\theta+c\theta^2)^2, \tag{31}$$

这里 $n\geqslant 0$，l，m 是整数。对（31）讨论可给出方程（30）仅有整数解$x=0$，-2，2，4，12。

此外，Avanesov[18]证明了Sierpinski的一个猜想，即

定理15 方程

$$\frac{y(y+1)}{2}=\frac{x(x+1)(x+2)}{6}=n$$

仅有正整数解$n=1,10,120,1540$和7140。

1971年，Ljunggren[19]还完满地回答了Mordell的一个

问题。Mordell问：方程

$$6y^2=(x+1)(x^2-x+6) \tag{32}$$

是否仅有整数解$x=-1,0,2,7,15,74$？Ljunggren证明了

定理16 方程（32）仅有整数解是 $x=-1,0,2,7,15,74$和767。

Mordell[20] 对于方程（1）的较为一般的情形，使用简单同余法还证明了一些结果。

定理17 设$a>0$，b，c是整数，d是奇的且没有$4k+3$形素因子。则方程

$$y^2=2ax^3+(6-2a-2c+8b)x^2+2cx-d^2 \tag{33}$$

的整数解满足$x<0$，$x\equiv 3 \pmod 4$。如果 $c=1-a+2b, d^2=1$，$a>0$，$3a>1+b$，则方程（33）仅有整数解（x,y）$=(-1,\pm 1)$；如果 $b=3a+1$，$c=5a+3$，$d^2=1$，$a>0$，则方程（33）仅有整数解 $(x,y)=(-1,\pm 1)$和$(-5,\pm 13)$。

证 如果$x\equiv 0 \pmod 2$，则由$2\nmid d$知（33）给出$y^2\equiv -1 \pmod 4$，而这不可能。如果 $x\equiv 1 \pmod 4$，则对（33）取模8得

$$y^2\equiv 2a+(6-2a-2c+8b)+2c-1\equiv 5 \pmod 8,$$

此也不可能。于是$x\equiv 3 \pmod 4$。由于（33）给出$y^2\equiv -d^2 \pmod x$，故在$x>0$时有奇素数$p\equiv 3 \pmod 4$使得$p\mid x$，$y^2\equiv -d^2 \pmod p$。由d不含$4k+3$形的素因子，知$p\nmid d$，于是有 $1=\left(\frac{-d^2}{p}\right)=\left(\frac{-1}{p}\right)=-1$矛盾。这就证明了$x<0$。

如果 $x\leqslant -5$，则在 $c=1-a+2b, d^2=1, 3a>1+b(a>0)$时易知

$$(x+1)(2ax^2+(4-2a+4b)x-2)<-1,$$

此给出$y^2<0$，这不可能。于是$x=-1$，$y=\pm 1$。在$b=3a+$

1，$c=5a+3$，$d^2=1(a>0)$时，（33）化为

$$y^2=2ax^3+(12a+8)x^2+(10a+6)x-1。\qquad (34)$$

设$x\leqslant -9$，改写（34）为

$$y^2-1=(x+1)(2ax^2+(10a+8)x-2)。$$

如果$a>1$，即 $9a>5a+4$，则有 $ax^2+(5a+4)x-1>0$，由此知上式给出 $y^2<0$，这不可能。如果$a=1$，则（34）给出

$$y^2=2x^3+20x^2+16x-1。$$

由$y^2\not\equiv -1(\mathrm{mod}3)$知 $x\neq -9$，所以 $x\leqslant -13$。但这时由于$x^2+10x+8>0$，故

$$y^2=2x(x^2+10x+8)-1<0,$$

仍不可能。于是$0>x>-9$。由$x\equiv 3(\mathrm{mod}4)$知$x=-1,-5$，代入（34）知分别给出$y=\pm 1$，± 13。证毕。

最近，Cassels[51] 证明了方程 $y^2=(x-1)^3+x^3+(x+1)^3=3x(x^2+2)$仅有整数解$x=0$，1，2和24。

§2　方程$x^3+b=Dy^n(n=2,3)$

1．丢番图方程$x^3+b=Dy^2$

对于丢番图方程

$$x^3+b=Dy^2,\ b\in\{\pm 1,\pm 8\} \qquad (1)$$

和

$$x^3+b=3Dy^2,\ b\in\{\pm 1,\ \pm 8\}, \qquad (2)$$

曾经有过不少研究工作。例如在$b=\pm 1$，$D=1$时，方程(1)化为Catalan方程（见第八章）的特例

$$x^3\pm 1=y^2。$$

Euler早已证明方程 $x^3+1=y^2$仅有正整数解 $x=2, y=3$；Lebesgue也在1850年证明了方程$x^3-1=y^2$无正整数解。对

于较为一般的情形，1924年前后Nagell[21][22]分别证明了如下的两个定理。

定理 1 设$D>1$且D仅被3或$12k+5$形的素数整除，则方程$x^3+1=Dy^2$仅有整数解$x=-1$，$y=0$。

定理 2 设二次域$Q(\sqrt{-D})$的类数h满足$h\neq 0 \pmod{3}$，则方程$x^3-1=Dy^2$没有$2\nmid x$的整数解。

1942年，Ljunggren[23]进一步地证明了

定理 3 设$D>2$，且D不被3或$6k+1$形素数整除，则(1)和(2)中的八个丢番图方程总共最多只有一组正整数解。

同时Ljunggren还证明了方程$x^3-1=23y^2$仅有整数解$x=1$，$y=0$以及方程$x^3-1=7y^2$仅有三组正整数解$(x,y)=(2,1)$，$(4,3)$，$(22,39)$。Nagell和Ljunggren的方法都不是初等的。

1952年，Ljunggren用Pell方程的初等方法给出了方程$x^3+1=2y^2$的一个初等解法。1972年，Vander Waall和Robert[24]也利用Pell方程法证明了方程$x^3-1=2y^2$仅有整数解$(x,y)=(1,0)$和方程$x^3+1=2y^2$仅有整数解$(x,y)=(1,\pm 1)$，$(-1,0)$，$(23,\pm 78)$。具有较大改进的是1981年柯召和孙琦[25][26]的工作，他们用Pell方程的方法证明了

定理 4 设$D>6$，且D不被$6k+1$形素数整除，则丢番图方程

$$x^3\pm 1=Dy^2 \qquad (3)$$

仅有$y=0$的整数解。

上面的这些定理没有给出方程$x^3\pm 1=3y^2$的全部解。最近，曹珍富和刘培杰[27]用分解因子法给出了定理4的更

为简洁的初等证明，而且连同$D=1,2,3,6$一起，方程（3）得到了统一处理，即有

定理 5 设$D>0$且不被$6k+1$形素数整除，则丢番图方程（3）除开$x^3+1=y^2$仅有正整数解$(x,y)=(2,3)$和$x^3+1=2y^2$仅有正整数解$(x,y)=(1,1)$，$(23,78)$外，其他均无正整数解。

证 先讨论丢番图方程

$$x^3-1=Dy^2。\quad (4)$$

设方程（4）有正整数解x,y。由于$(x-1,x^2+x+1)=1$或3，且素数$p\equiv5(\mathrm{mod}\,6)$或$p=2$满足$p\nmid x^2+x+1$，故由(4)得出

$$x-1=Dy_1^2,\quad x^2+x+1=y_2^2,\quad (5)$$

或

$$x-1=3Dy_1^2,\quad x^2+x+1=3y_2^2,\quad (6)$$

这里$y_1>0$，$y_2>0$且$(y_1,y_2)=1$。（5）由第二式整理得$(2x+1)^2+3=4y_2^2$，故$2y_2\pm(2x+1)=1$，$2y_2\mp(2x+1)=3$，从而$y_2=1$，$x=0$或-1，非原方程的正整数解。

对于（6）式，由$x=3Dy_1^2+1$代入$x^2+x+1=3y_2^2$得

$$(2y_2)^2-1=3(2Dy_1^2+1)^2,$$

由此得出

$$2y_2-1=3y_3^2,\ 2y_2+1=y_4^2,\ 2Dy_1^2+1=y_3y_4,\quad (7)$$

或

$$2y_2-1=y_3^2,\ 2y_2+1=3y_4^2,\ 2Dy_1^2+1=y_3y_4,\quad (8)$$

其中$y_3>0$，$y_4>0$且$(y_3,y_4)=1$。对（7），由于$2\nmid y_3y_4$，故由

$$2y_2=3y_3^2+1=y_4^2-1$$

取模8知不成立。对(8)，由前两式得$y_3^2-3y_4^2=-2$，故

由$2Dy_1^2+1=y_3y_4$得出

$$4Dy_1^2=2y_3y_4-2=2y_3y_4+y_3^2-3y_4^2$$
$$=(y_3-y_4)(y_3+3y_4)。\qquad (9)$$

如果$2|D$或$2|y_1$，则由$2Dy_1^2+1=y_3y_4$知$y_3\equiv y_4(\mathrm{mod}4)$，故$(y_3-y_4,\ y_3+3y_4)=4$，所以(9)给出

$$y_3-y_4=4D_1y_5^2,\quad y_3+3y_4=4D_2y_6^2,\quad D=D_1D_2,$$

其中$y_1=2y_5y_6$，$y_5>0$，$y_6>0$ 且$(y_5,\ y_6)=1$。现由上式的前两式解出

$$y_3=3D_1y_5^2+D_2y_6^2,\quad y_4=D_2y_6^2-D_1y_5^2,$$

代入$y_3^2-3y_4^2=-2$得

$$4(D_2y_6^2)^2-3(D_1y_5^2+D_2y_6^2)^2=1。\qquad (10)$$

显然$2\nmid D_2$，$3\nmid D_2$。由假设知，若$D_2>1$,则D_2含有$6k+5$形的素因子p。但$\left(\frac{-3}{p}\right)=-1$，故(10)给出$D_2=1$。于是(10)化为

$$4y_6^4-3(Dy_5^2+y_6^2)^2=1。\qquad (11)$$

我们将在第七章证明(11)仅有$y_6^2=Dy_5^2+y_6^2=1$，给出$y_5=0$，与$y_5>0$矛盾。

如果$2\nmid D$且$2\nmid y_1$，则由$2Dy_1^2+1=y_3y_4$知$y_3y_4\equiv 3(\mathrm{mod}4)$,即$y_3-y_4\equiv 2(\mathrm{mod}4)$。所以$(y_3-y_4, y_3+3y_4)=2$，故(9)给出

$$y_3-y_4=2D_1y_5^2,\quad y_3+3y_4=2D_2y_6^2, D=D_1D_2,\qquad (12)$$

其中$y_1=y_5y_6$，$y_5>0$，$y_6>0$且$(y_5,\ y_6)=1$。由(12)解出$y_3=\frac{3D_1y_5^2+D_2y_6^2}{2}$，$y_4=\frac{D_2y_6^2-D_1y_5^2}{2}$，代入$y_3^2-3y_4^2=-2$得

$$(D_2y_6^2)^2-3\left(\frac{D_1y_5^2+D_2y_6^2}{2}\right)^2=1。\qquad (13)$$

由于$2\nmid D$，故$2\nmid D_2$，且(13)给出$3\nmid D_2$，故而知 $D_2=1$。由第七章方程 $x^4-3y^2=1$ 仅有整数解 $x=\pm 1$，$y=0$ 知，(13)给出 $y_1^2=1$，$\frac{Dy_5^2+y_6^2}{2}=0$，这也不可能。

与上面完全类似地，可以证明方程 $x^3+1=Dy^2$ 的结果。证毕。

对于$b=\pm 8$，由方程(1)和(2)得

$$x^3\pm 8=Dy^2,\quad x^3\pm 8=3Dy^2(D>0)。\tag{14}$$

由定理3知，在$D>2$且不被3或$6k+1$形素数整除时，(14)中的四个丢番图方程总共最多只有一组正整数解。因此，对某D(满足定理 3 条件)，如果找到(14)中的一个方程的一组正整数解，则(14)便全部得到解决。例如方程 $x^3-8=55y^2$有解$x=167$，$y=291$，故$x^3+8=55y^2$和$x^3\pm 8=165y^2$ 均无正整数解，且方程$x^3-8=55y^2$仅有正整数解 $x=167$，$y=291$。

1981年，柯召和孙琦[28]证明了

定理 6 设$D>2$ 无平方因子且不被3或$6k+1$形的素数整除，则丢番图方程

$$x^3+8=Dy^2\tag{15}$$

在$D\not\equiv 1(\bmod 4)$时仅有整数解 $x=-2$，$y=0$；而丢番图方程

$$x^3-8=Dy^2\tag{16}$$

在$D\not\equiv 3(\bmod 4)$时仅有整数解$x=2$，$y=0$。

定理 7 设$D>2$无平方因子且不被3或 $6k+1$ 形的素数整除，则丢番图方程

$$x^3+8=3Dy^2\tag{17}$$

在$D\not\equiv 11,\ 19(\bmod 20)$ 时仅有整数解 $x=-2$，$y=0$；而丢

番图方程

$$x^3-8=3Dy^2 \tag{18}$$

在$D\neq 1$，9(mod20)时仅有整数解$x=2$，$y=0$。

现在给出定理6、7的证明：设$d=D$或$3D$，先讨论方程(15)和(17)，即有

$$x^3+8=dy^2。 \tag{19}$$

如果$2|x$，则(19)化为方程(3)的情形，此时由定理4知仅给出$x=-2$，$y=0$。如果$2\nmid x$，则(19)给出$2\nmid d$，$2\nmid y$。此时不妨设$x>0$，$y>0$，由于$(x+2,x^2-2x+4)=1$或3，且如是后者，则$3\|x^2-2x+4$。因此由D从而d的假设知，(19)给出

$$x+2=du^2,\quad x^2-2x+4=v^2,\quad y=uv,\quad u>0,\quad v>0, \tag{20}$$

或

$$x+2=3du^2,\quad x^2-2x+4=3v^2, y=3uv, u>0, v>0。 \tag{21}$$

由(20)的第二式得$(x-1)^2+3=v^2$，由于$2\nmid x$，故此给出$3\equiv 1 \pmod 4$的矛盾结果。现由(21)的前两式消去x得

$$3d^2u^4-6du^2+4=v^2,$$

由此即得

$$v^2-3(du^2-1)^2=1。 \tag{22}$$

(22)是一个Pell方程。熟知方程$x^2-3y^2=1$的基本解$\varepsilon=2+\sqrt{3}$，令$\bar{\varepsilon}=2-\sqrt{3}$，则(22)给出

$$v=\frac{\varepsilon^s+\bar{\varepsilon}^s}{2},\quad du^2-1=\frac{\varepsilon^s-\bar{\varepsilon}^s}{\varepsilon-\bar{\varepsilon}},\quad s>0 \tag{23}$$

因为$2\nmid x$时(21)给出$2\nmid v$，故(23)的第一式推得$2|s$。设$s=2t$，$t>0$，则(23)的第二式成为

$$du^2-1=\frac{\varepsilon^{2t}-\bar{\varepsilon}^{2t}}{\varepsilon-\bar{\varepsilon}},\quad t>0。 \tag{24}$$

因为$\frac{\varepsilon^{2t}-\bar{\varepsilon}^{2t}}{\varepsilon^2-\bar{\varepsilon}^2}$是整数，故 $\varepsilon+\bar{\varepsilon}=4 \Big| \frac{\varepsilon^{2t}-\bar{\varepsilon}^{2t}}{\varepsilon-\bar{\varepsilon}}$，因此(24)给出$d\equiv 1 \pmod 4$。故在 $d=D\not\equiv 1 \pmod 4$ 时，方程(15)仅有整数解 $x=-2$，$y=0$。而在$d=3D$时，必有$D\equiv 3 \pmod 4$，而且我们将证明此时(24)还给出$D\equiv 1,4 \pmod 5$。

易知 $\varepsilon^2+\varepsilon\bar{\varepsilon}+\bar{\varepsilon}^2=15$，设$n\geqslant 6$，由

$$\frac{\varepsilon^n-\bar{\varepsilon}^n}{\varepsilon-\bar{\varepsilon}}-\frac{\varepsilon^{n-6}-\bar{\varepsilon}^{n-6}}{\varepsilon-\bar{\varepsilon}}=(\varepsilon^{n-3}+\bar{\varepsilon}^{n-3})\left(\frac{\varepsilon^3-\bar{\varepsilon}^3}{\varepsilon-\bar{\varepsilon}}\right)$$

知

$$\frac{\varepsilon^n-\bar{\varepsilon}^n}{\varepsilon-\bar{\varepsilon}}\equiv\frac{\varepsilon^{n-6}-\bar{\varepsilon}^{n-6}}{\varepsilon-\bar{\varepsilon}} \pmod{15}。 \qquad (25)$$

在(24)中，如果$3|t$，则(24)给出 $du^2-1\equiv 0 \pmod 3$，但此时 $d=3D$，故不可能；如果$t=3t_1+1$，$t_1\geqslant 0$，则由(24)，(25)得（注意 $d=3D$）

$$3Du^2-1=\frac{\varepsilon^{6t_1+2}-\bar{\varepsilon}^{6t_1+2}}{\varepsilon-\bar{\varepsilon}}\equiv\varepsilon+\bar{\varepsilon}\equiv 1 \pmod 3,$$

此仍不可能；剩下的可能是$t=3t_1+2$，$t_1\geqslant 0$,此时由(24)，(25)得

$$3Du^2-1=\frac{\varepsilon^{6t_1+4}-\bar{\varepsilon}^{6t_1+4}}{\varepsilon-\bar{\varepsilon}}\equiv\frac{\varepsilon^4-\bar{\varepsilon}^4}{\varepsilon-\bar{\varepsilon}}\equiv 1 \pmod 5,$$

此给出$\left(\frac{D}{5}\right)=1$，故 $D\equiv 1, 4 \pmod 5$。于是在 $D\not\equiv 11, 19 \pmod{20}$时，方程(17)仅有整数解$x=-2$，$y=0$。

同样方法，可证方程(16)和(18)的结果。证毕。

由定理5、6的证明过程和定理 7 可推出，方程 $x^3-8=y^2$，$x^3-8=2y^2$，$x^3+8=3y^2$和$x^3\pm 8=6y^2$均仅有 $y=0$ 的整数解。而$x^3+8=2y^2$仅有正整数解 $x=4$，$y=6$。剩下

$x^3+8=y^2$和$x^3-8=3y^2$没有解决。显然方程$x^3-8=3y^2$有正整数解$x=11$，$y=21$。而方程$x^3+8=y^2$也有正整数解$(x,y)=(1,3)$，$(2,4)$，$(46,312)$。我们来证明

定理 8 丢番图方程

$$x^3-8=3y^2 \tag{26}$$

仅有正整数解$x=11$，$y=21$。

证 设x，y是(26)的正整数解，则由定理5知 $2\nmid x$，故由(26)得出

$$x-2=9y_1^2,\quad x^2+2x+4=3y_2^2,\quad y=3y_1y_2,\quad 2\nmid y_1y_2。\tag{27}$$

由(27)的前两式整理得

$$y_2^2-3(3y_1^2+1)^2=1,\quad 2\nmid y_1y_2,$$

由此即知

$$3y_1^2+1=\frac{\varepsilon^{2t}-\bar{\varepsilon}^{2t}}{2\sqrt{3}},\quad t>0,$$

这里$\varepsilon=2+\sqrt{3}$，$\bar{\varepsilon}=2-\sqrt{3}$。故由$\left(\frac{\varepsilon^t+\bar{\varepsilon}^t}{2}\right)^2-3\left(\frac{\varepsilon^t-\bar{\varepsilon}^t}{2\sqrt{3}}\right)^2=1$知

$$\begin{aligned}3y_1^2&=2\left(\frac{\varepsilon^t-\bar{\varepsilon}^t}{2\sqrt{3}}\right)\left(\frac{\varepsilon^t+\bar{\varepsilon}^t}{2}\right)+3\left(\frac{\varepsilon^t-\bar{\varepsilon}^t}{2\sqrt{3}}\right)^2-\left(\frac{\varepsilon^t+\bar{\varepsilon}^t}{2}\right)^2\\&=\left(3\cdot\frac{\varepsilon^t-\bar{\varepsilon}^t}{2\sqrt{3}}-\frac{\varepsilon^t+\bar{\varepsilon}^t}{2}\right)\left(\frac{\varepsilon^t-\bar{\varepsilon}^t}{2\sqrt{3}}+\frac{\varepsilon^t+\bar{\varepsilon}^t}{2}\right)\\&=\left(\frac{\lambda^{2t+1}+\bar{\lambda}^{2t+1}}{2^t}\right)\left(\frac{\lambda^{2t+1}-\bar{\lambda}^{2t+1}}{2^{t+1}\sqrt{3}}\right),\end{aligned}\tag{27'}$$

其中$\lambda=1+\sqrt{3}$，$\bar{\lambda}=1-\sqrt{3}$，$\lambda\bar{\lambda}=-2$。由于

$$\left(\frac{\lambda^{2t+1}+\bar{\lambda}^{2t+1}}{2^t},\frac{\lambda^{2t+1}-\bar{\lambda}^{2t+1}}{2^{t+1}\sqrt{3}}\right)\Bigg|\,4\left(\frac{\varepsilon^t+\bar{\varepsilon}^t}{2},\frac{\varepsilon^t-\bar{\varepsilon}^t}{2\sqrt{3}}\right)=4,$$

而$2\nmid y_1$，$3\nmid \frac{\lambda^{2t-1}+\bar{\lambda}^{2t-1}}{2^t}$，故(27′)给出

$$\frac{\lambda^{2t-1}+\bar{\lambda}^{2t-1}}{2^t}=u^2,\quad \frac{\lambda^{2t-1}-\bar{\lambda}^{2t-1}}{2^{t+1}\sqrt{3}}=3v^2,\ y_1=uv。\tag{28}$$

现由(28)的第二式知

$$\left(\frac{\lambda^{2t+1}+\bar{\lambda}^{2t+1}}{2^{t+1}}\right)^2-27v^4=-2,$$

此由第二章§7的例1知，仅有$\frac{\lambda^{2t+1}+\bar{\lambda}^{2t+1}}{2^{t+1}}=5$，$v^2=1$，故$t=1$，于是(28)给出$y_1=1$，由(27)知 $x=11$，$y=21$。证毕。

利用方程$x^4-3y^2=-2$，$x^2-3y^4=-2$以及$x^2-27y^4=-2$的结果，可以给出更多的形为$x^3+b=Dy^2(b=\pm 8)$的丢番图方程的解。利用递推序列的方法，很容易证明方程$x^4-3y^2=-2$和$x^2-3y^4=-2$都仅有唯一的正整数解$(x,y)=(1,1)$。我们认为，利用递推序列的方法（参阅第二章§7）能够给出在$D>0$且D不被$6k+1$形的素数整除时，方程(15)、(16)、(17)和(18)的全部整数解。因此有如下的猜想：设$D>0$且D不被$6k+1$形的素数整除，则最多只有有限个D使得丢番图方程

$$x^3\pm 8=Dy^2$$

有正整数解。

最后，由于编码理论的需要，1982 年 Bremner 和 Morton[29]提出了解丢番图方程

$$y^2=4cx^3+13(c=1,3,9)\tag{28′}$$

的问题。利用代数数论和p-adic 方法不难给出(28′)的全部

解。例如，在 $Q(\sqrt{13})$ 中分解（28′）式为

$$\left(\frac{y+\sqrt{13}}{2}\right)\left(\frac{y-\sqrt{13}}{2}\right)=cx^3\ (c=1,3,9)。\tag{29}$$

在$c=1$时，（29）给出

$$\frac{y+\sqrt{13}}{2}=\varepsilon^k\left(a+b\frac{1+\sqrt{13}}{2}\right)^3,\ k=0,\ \pm1,\tag{30}$$

这里 $\varepsilon=\frac{3+\sqrt{13}}{2}$是 $Q(\sqrt{13})$的基本单位数，a,b是有理整数。在$c=3$时，(29)给出

$$\frac{y+\sqrt{13}}{2}=\varepsilon^k\frac{1\pm\sqrt{13}}{2}\left(a+b\frac{1+\sqrt{13}}{2}\right)^3,\ k=0,\pm1,\tag{31}$$

而在$c=9$时，（29）给出

$$\frac{y+\sqrt{13}}{2}=\varepsilon^k\left(\frac{1\pm\sqrt{13}}{2}\right)^2\left(a+b\frac{1+\sqrt{13}}{2}\right)^3,$$

$$k=0,\ \pm1。\tag{32}$$

对(30)，在$k=0$时显然不可能，而在$k=1$和-1时分别给出

$$a^3+6a^2b+15ab^2+11b^3=1,\tag{33}$$

$$a^3-3a^2b+6ab^2-b^3=1。\tag{34}$$

在(33)和(34)中分别令 $(X,Y)=(a+2b,b)$和$(a-b,b)$，则都可化为

$$X^3+3XY^2-3Y^3=1。$$

此由第三章§3的例 2 知仅有$(X,Y)=(1,0)$和$(1,1)$的整数解。由此推出$c=1$时方程(28′)仅有整数解$(x,y)=(-1,\pm3)$和$(3,\pm11)$。利用p-adic方法还可给出(31)和(32)的全部解。

Ⅱ. 丢番图方程 $x^3+b=Dy^3$

我们在第三章的§3中，证明了丢番图方程

$$x^3+1=Dy^3,\ D>1,\ xy\neq 0 \tag{35}$$

最多只有一组整数解x，y。由代数数论知，如果 x_1，y_1是(35)的一组解，则 $x_1+y_1\sqrt[3]{D}$或者是三次域$Q(\sqrt[3]{D})$的基本单位数，或者是基本单位数的平方。因此，定出哪些D使方程（35）有解或无解是一件有意义的工作。1967 年，Cohn[36]证明了

定理 9 方程(35)在条件1)～3)时分别没有整数解：

1) 在$D\equiv 0 \pmod 9$时，除$D=9$和D有某个分解$D=pq$，p,q是正整数，满足

(*a*) $(p,q)=1$，$p\neq p_1^3$；

(*b*) 如果$p_1 \mid p$，则$p_1\equiv 1 \pmod 6$；

如果$D\equiv 0 \pmod{27}$，则必须加上

(*c*) $p\equiv 1 \pmod{18}$。

2) 在$D\equiv \pm 3$或$\pm 4 \pmod 9$时，除$D=pq$，p，q是正整数满足(*a*)、(*b*)和(*c*)。

3) 在$D\equiv \pm 1$或$\pm 2 \pmod 9$时，除$D=1,2,17,20,5831$和6860，和$D=pq$，p,q是正整数满足(*a*)、(*b*)和(*c*)。

1971年，Bernstein[31]证明了

定理10 如果$D=d^3+k$，$|k|\neq 1$，$k\in\{K,3K,3d,6d,-K,-3K\}$，这里$K\mid d$，则除开$D=20$($k=6d$，$d=2$)，方程(35)有解$x=19$，$y=7$外，其他情形(35)均无整数解。

后来，曹珍富与曹玉书[32]证明了

定理11 设D不被$6k+1$形的素数整除，则丢番图方程(35)除开$D=2$仅有解$(x,y)=(1,1)$，$D=9$仅有解$(x,y)=(2,1)$，$D=17$仅有解$(x,y)=(-18,-7)$和$D=20$仅有解$(x,y)=(-19,-7)$外，其它情形均无整数解。

这个定理的证明将用到方程$x^2+x+1=y^3$ 仅有整数解$(x,y)=(0,1)$，$(-1,1)$，$(18,7)$ 和 $(-19,7)$ 以及方程$x^2+x+1=3y^3$仅有整数解$(x,y)=(1,1)$ 和 $(-2,1)$的结论。前一结论是 Ljunggren[33] 在1942年得到的，而后一结论的证明将依赖于方程$x^3+y^3=z^3$（此在本章§4中给出），因为$x^2+x+1=3y^3$可整理成$(x+2)^3-(x-1)^3=(3y)^3$。

对于丢番图方程

$$x^3+8=Dy^3,\quad D>1,\quad xy\neq 0, \tag{36}$$

我们有

定理12 设D不被$6k+1$形的素数整除，则丢番图方程(36)除开$D=2$仅有解$(x,y)=(2,2)$，$D=9$仅有解$(x,y)=(1,1)$和$(4,2)$，$D=16$仅有解$(x,y)=(2,1)$，$D=17$仅有解$(x,y)=(-36,-14)$，$D=20$仅有解$(x,y)=(38,14)$，$D=72$ 仅有解 $(x,y)=(4,1)$，$D=136$ 仅有解 $(x,y)=(-36,-7)$，$D=160$仅有解$(x,y)=(38,7)$ 外，其它情形均无整数解。

证 如果$2|x$，$2|y$则(36)化为

$$\left(\frac{x}{2}\right)^3+1=D\left(\frac{y}{2}\right)^3,\quad D>1,\quad xy\neq 0,$$

此由定理11知，仅当$D=2,9,17,20$时有解。如果$2|x,2\nmid y$，则由(36)知$2^3|D$。令$D=8d$，则(36)化为

$$\left(\frac{x}{2}\right)^3+1=dy^3,$$

此由定理11知，仅当$d=2,9,17,20$即$D=16,72,136,160$ 时有解。这两种情形分别给出定理 12 中除 $D=9$，$(x,y)=(1,1)$外相应的解。

如果$2\nmid x$，由于 $(x+2,x^2-2x+4)=1$或3，故与 I 的讨论类似，(36)给出

$$x^2-2x+4=y_1^3, \tag{37}$$

或

$$x^2-2x+4=3y_1^3, \tag{38}$$

这里$y_1|y$。对(37)，我们整理得

$$(x-1)^2+3=y_1^3, \tag{39}$$

由于$2\nmid x$，故对(39)取模4知$y_1\equiv 3(\bmod 4)$。改写(39)为

$$(x-1)^2+4=y_1^3+1\equiv 0(\bmod y_1^2-y_1+1),$$

而$y_1\equiv 3(\bmod 4)$推出 $y_1^2-y_1+1\equiv 3(\bmod 4)$，故上式不可能。这就证明了(37)不成立。

对(38)，可整理得

$$y_1^3-1=3\left(\frac{x-1}{3}\right)^2,$$

此由定理5知，仅有 $x=1$，$y_1=1$，故给出$D=9$，$y=1$。证毕。

对于一般的情形，Nagell[34]和Ljunggren[35]证明了一个重要的结果，即

定理13 设$c=1,3,a>b>1$是整数，$(ab,c)=1$ 且如果$c=3$，则可取$b=1$。则丢番图方程

$$ax^3+by^3=c \tag{40}$$

除开$2x^3+y^3=3$有两组解$(x,y)=(1,1)$和$(4,-5)$外，最多只有一组整数解x,y,并且对这样的解 $x,y,c^{-1}(x\sqrt[3]{a}+y\sqrt[3]{b})$是三次域$Q(\sqrt[3]{D})(=Q(\sqrt[3]{ab^2}))$的基本单位数或基本单位数的平方。

§3 二元三次型及其相关方程

一个二元三次型$f(x,y)$是指

$$f(x,y)=ax^3+bx^2y+cxy^2+dy^3, \tag{1}$$

这里a,b,c和d均是整数，且判别式

$$D=-27a^2d^2+18abcd+b^2c^2-4ac^3-4b^3d, \tag{2}$$

这里假设$D\neq0$。定义$H(x,y)$，$G(x,y)$如下：

$$H(x,y)=-\frac{1}{4}\begin{vmatrix}\frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x\partial y}\\ \frac{\partial^2 f}{\partial x\partial y} & \frac{\partial^2 f}{\partial y^2}\end{vmatrix}$$

$$=(bx+cy)^2-(3ax+by)(cx+3dy)$$

$$=Ax^2+Bxy+Cy^2, \tag{3}$$

这里 $A=b^2-3ac$，$B=bc-9ad$，$C=c^2-3bd$，且容易验证$H(x,y)$的判别式为$B^2-4AC=-3D$。

$$G(x,y)=\begin{vmatrix}\frac{\partial f}{\partial x} & \frac{\partial f}{\partial y}\\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y}\end{vmatrix}$$

$$=-(27a^2d-9abc+2b^3)x^3+\cdots。 \tag{4}$$

直接验证可有

$$G^2(x,y)+27Df^2(x,y)=4H^3(x,y)。 \tag{5}$$

利用(5)式，可以给出方程

$$X^2+kY^2=Z^3,\ (X,Z)=1 \tag{6}$$

的全部整数解，这是Mordell[2]得到的。

定理 1 丢番图方程(6)的全部整数解可表为

$$X=\frac{1}{2}G(x,y),\ Y=f(x,y),\ Z=H(x,y), \tag{7}$$

这里 $f(x,y)=ax^3+3bx^2+3cxy^2+dy^3$ 是任意的判别式$D=4k$的二元三次型，$H(x,y)=(b^2-ac)x^2+(bc-ad)xy+$

$(c^2-bd)y^2$，$G(x,y)=\frac{1}{3}\begin{vmatrix}\frac{\partial f}{\partial x} & \frac{\partial f}{\partial y}\\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y}\end{vmatrix}$，而 x,y 取使 $\left(\frac{1}{2}G(x,y),\ H(x,y)\right)=1$ 的任意整数。

证 首先由 $f(x,y)$，$H(x,y)$ 和 $G(x,y)$ 的表达式及(5)容易验证（见证明的后部分），$(\frac{1}{2}G(x,y))^2+kf^2(x,y)=H^3(x,y)$。现设 $X=g$，$Y=f$，$Z=h$ 是方程(6)的一个解，即有

$$g^2+kf^2=h^3,\ (g,h)=1。\qquad (8)$$

因为(8)式给出 $-k$ 是 h 的二次剩余，所以存在一个首项系数为 h，判别式为 $-4k$ 的二元二次型，设为

$$F(x,y)=hx^2+2Bxy+Cy^2,$$

这里 $B^2-hC=-k$。我们取 B 满足同余式 $fB\equiv-g(\bmod h^3)$，借助于 $F(x,y)$，我们构造一个判别式 $D=4k$ 的二元三次型 $f(x,y)=fx^3+3bx^2y+3cxy^2+dy^3$，且 $H(x,y)=F(x,y)=hx^2+2Bxy+Cy^2$，这里 $h=b^2-fc$，$2B=bc-fd$，$C=c^2-bd$。因为

$$h=b^2-fc,\ c=\frac{b^2-h}{f},$$

取 $b\equiv\frac{g}{h}(\bmod f)$，

$$bh=g+Bf\Rightarrow b\equiv0(\bmod h^2)。$$

于是

$$h^2c=\frac{(g+Bf)^2-h^3}{f}=-kf+2gB+B^2f。$$

我们来定出d。因为$bc-fd=2B$，有

$$fd=\left(\frac{-g+Bf}{h}\right)\left(\frac{-kf+2gB+B^2f}{h^2}\right)-2B,$$

推出

$$h^3d=-kg-3kfB+3gB^2+fB^3。$$

我们来证明c和d均为整数。由

$$h^2c\equiv -kf+2g\left(-\frac{g}{f}\right)+\frac{g^2}{f}(\bmod h^2)$$

$$\equiv\frac{-kf^2-g^2}{f}\equiv 0(\bmod h^2)$$

知$c\equiv 0(\bmod 1)$，故c是整数；同样，由

$$h^3d\equiv -kg+3kg+\frac{3g^3}{f^2}-\frac{g^3}{f^2}(\bmod h^3)$$

$$\equiv\frac{2g}{f^2}(kf^2+g^2)\equiv 0(\bmod h^3)$$

知d是整数。

由于$f(x,y)=fx^3+3bx^2y+3cxy^2+dy^3$的判别式为$27D$，$D=-f^2d^2+6fbcd+3b^2c^2-4fc^3-4db^3=4k$，由(3)式、(4)式定义的$H_1(x,y)$和$G_1(x,y)$分别为

$$H_1(x,y)=9H(x,y),$$

$$G_1(x,y)=27G(x,y),$$

这里$G(x,y)=-(f^2d-3fbc+2b^3)x^3+\cdots$。故由(5)式知

$$G_1^2(x,y)+(27)^2Df^2(x,y)=4H_1^3(x,y),$$

从而

$$G^2(x,y)+Df^2(x,y)=4H^3(x,y)。$$

由$D=4k$知，$2\mid G(x,y)$，故上式给出

$$\left(\frac{1}{2}G(x,y)\right)^2+kf^2(x,y)=H^3(x,y)。$$证毕。

方程（6）的结果可以用于解前两节中的某些丢番图方程。例如在定理1中令$X=\pm1$，则(6)式化为

$$Z^3-1=kY^2, \tag{9}$$

此时只要解方程

$$G(x,y)=\pm2。$$

再如令$Y=\pm1$，则(6)化为

$$X^2+k=Z^3,\ (X,Z)=1, \tag{10}$$

此时只要解方程

$$f(x,y)=\pm1。$$

利用Thue定理（见第三章§4）可知，方程(9)和(10)在某些情况下均只有有限个整数解X，Y。Mordell[2] 还给出对所有k，方程(10)均只有有限组解（是§1中定理1的推论）。

对于给定的二元三次型$f(x,y)$，研究丢番图方程

$$f(x,y)=1 \tag{11}$$

的解是比较困难的，尤其是在 $f(x,y)$ 的判别式$D>0$的时候。设$f(\theta,1)=0$，在三次域$Q(\theta)$中，如果 $D\leqslant0$，则利用p-adic 方法十分容易求解，这是因为这时三次域$Q(\theta)$中只有一个基本单位数。如果$D>0$，则三次域$Q(\theta)$中有两个基本单位数，这时处理起来十分地麻烦，而且许多都需要使用丢番图逼近方法。有些特殊的情形，利用第三章§3的方法和特殊的技巧，才有希望给以解决。目前，在$D>0$时只解决了几个特例：

1)[36]　$D=49$，方程$x^3+x^2y-2xy^2-y^3=1$仅有解(1,0)，(0,1)，(−1,1)，(5,4)，(4,−9)，(−9,5)，(2,−1)，(−1,−1)和(−1,2)；

2)[33]　$D=81$，方程$x^3-3xy^2+y^3=1$仅有解(1,0)，(0,−1)，(−1,1)，(2,1)，(−3,2)和(1,−3)；

3)[6]　$D=148$，方程$x^3-4xy^2+2y^3=1$仅有解$(-1,-1)$，$(1,0)$，$(1,2)$，$(-5,3)$和$(-31,14)$；

4)[5]　$D=3024$，方程 $x^3-12xy^2-12y^3=1$ 仅有解$(1,0)$和$(1,-1)$。

一般情形，Siegel[37]证明了

定理 2　如果D是充分大的正整数，则方程$f(x,y)=1$最多有8个整数解。

现在我们用丢番图逼近的方法给出4)的一个证明。设$f(x,y)=x^3-12xy^2-12y^3$，$f(\theta,1)=0$，在三次域$Q(\theta)$中，整底是1，θ，$\frac{1}{2}\theta^2$，基本单位数是

$$\eta_1=-7-4\theta+\frac{3}{2}\theta^2,\quad \eta_2=11+\theta-\theta^2。$$

由于$f(x,y)=1$推出

$$(x-\theta^{(1)}y)(x-\theta^{(2)}y)(x-\theta^{(3)}y)=1。$$

令 $\beta=x-\theta y$，$\theta\in\{\theta^{(1)},\ \theta^{(2)},\ \theta^{(3)}\}$，则$\beta$ 是 $Q(\theta)$ 中的单位，因而$\beta=\pm\eta_1{}^{b_1}\eta_2{}^{b_2}$，$b_1$，$b_2\in Z$。于是

$$\log|\beta^{(j)}|=b_1\log|\eta_1{}^{(j)}|+b_2\log|\eta_2{}^{(j)}|,\quad 1\leqslant j\leqslant 3$$

推出

$$b_r=\frac{1}{\triangle}\{\log|\beta^{(j)}|\cdot\log|\eta_s^{(i)}|-\log|\beta^{(i)}|\cdot\log|\eta_s^{(j)}|\},$$

$$r,\ s\in\{1,2\}\ (r\neq s),$$

这里

$$\triangle=\log|\eta_1{}^{(j)}|\cdot\log|\eta_2{}^{(i)}|-\log|\eta_1{}^{(i)}|\cdot\log|\eta_2{}^{(j)}|。$$

如果$H=\max\{|b_1|,\ |b_2|\}$，$M=\max\{\log|\eta_1{}^{(i)}|,\log|\eta_2{}^{(i)}|\}$，我们有

$$H\leqslant\frac{1}{|\triangle|}\{|\log|\beta^{(j)}|+\log|\beta^{(i)}||\}\cdot M。$$

因此$\max\{\log|\beta^{(i)}|\}\geqslant\frac{|\Delta|}{2M}\cdot H=\delta\cdot H$。为了便于使用，我们给出若干计算结果：方程$f(\theta,1)=0$的三个根是

$$\theta^{(1)}=-2.768734305276282\cdots,$$

$$\theta^{(2)}=-1.115749396663048\cdots,$$

$$\theta^{(3)}=3.884483701939\,33\cdots,$$

基本单位数η_1，η_2分别是方程$x^3-15x^2-9x+1=0$和$x^3-9x^2+3x+1=0$的根，相应地有

$$\eta_1^{(1)}=15.573771700925751\,0\cdots;$$

$$\eta_2^{(1)}=0.565376041509972\cdots;$$

$$\eta_1^{(2)}=-0.669557339116867\,8\cdots;$$

$$\eta_2^{(2)}=8.639353887182992\cdots;$$

$$\eta_1^{(3)}=0.095885638191116\,8\cdots;$$

$$\eta_2^{(3)}=-0.204729928692964\,2\cdots;$$

$$\log|\eta_1^{(1)}|=2.745588198059661\cdots,$$

$$\log|\eta_2^{(1)}|=-0.570264209028009\,2\cdots,$$

$$\log|\eta_1^{(2)}|=-0.400989131578108\,9\cdots,$$

$$\log|\eta_2^{(2)}|=2.156327798443639\cdots,$$

$$\log|\eta_1^{(3)}|=-2.344599066481552\cdots,$$

$$\log|\eta_2^{(3)}|=-1.586063589415630\cdots,$$

$$\max_i\Big|\,|\log|\eta_1^{(i)}||-|\log|\eta_2^{(i)}||\,\Big|$$

$$=2.175323989031652\cdots,$$

$$\log\left|\frac{\eta_1^{(1)}}{\eta_1^{(3)}}\right|=5.090187264541213\cdots,$$

$$\log\left|\frac{\eta_1^{(2)}}{\eta_1^{(3)}}\right|=1.943609934903443\cdots,$$

$$\log\left|\frac{\eta_1^{(1)}}{\eta_1^{(2)}}\right| = 3.146577329637770\cdots,$$

$$\log\left|\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right| = 2.762592007471648\cdots,$$

$$\log\left|\frac{\eta_2^{(2)}}{\eta_2^{(3)}}\right| = 3.742391387859269\cdots,$$

$$\log\left|\frac{\eta_2^{(1)}}{\eta_2^{(3)}}\right| = 1.015799380387621\cdots,$$

$$|\theta^{(1)}-\theta^{(2)}| = 1.652984908613233\cdots,$$

$$|\theta^{(1)}-\theta^{(3)}| = 6.653218007215614\cdots,$$

$$|\theta^{(3)}-\theta^{(2)}| = 5.00023309860238\cdots,$$

$$\log|\theta^{(1)}-\theta^{(2)}| = 0.5025826891016480\cdots,$$

$$\log|\theta^{(1)}-\theta^{(3)}| = 1.895100648480152\cdots,$$

$$\log|\theta^{(3)}-\theta^{(2)}| = 1.60948453106791\cdots,$$

$$\max_{k\neq l}\left|\frac{\theta^{(i)}-\theta^{(k)}}{\theta^{(l)}-\theta^{(k)}}\right| \leqslant e^{\alpha},\quad \alpha = 1.392517959378504\cdots。$$

这里 l 是最小的使 $\log|\beta^{(l)}| \leqslant -\frac{1}{2}\delta H$。由于$M = 2.745588\cdots$，$|\triangle| = 2.15632779\cdots$，故 $\delta \geqslant 2.6730415\cdots$。因为 $\log|\beta^{(1)}| + \log|\beta^{(2)}| + \log|\beta^{(3)}| = 0$，故 l 是存在的，只是我们不知道哪个 l 使 $\log|\beta^{(l)}| \leqslant -\frac{1}{2}\delta H$。这样，我们就得计算3个可能的 l 值。由

$$|\beta^{(1)}|\cdot|\beta^{(2)}|\cdot|\beta^{(3)}| = 1 \Rightarrow |\beta^{(k)}|\cdot|\beta^{(i)}| = |\beta^{(l)}|^{-1} \geqslant \exp\left(\frac{1}{2}\delta H\right),$$

不妨设 $|\beta^{(i)}| \leqslant |\beta^{(k)}|$，则得出 $|\beta^{(k)}| \geqslant \exp\left(\frac{1}{4}\delta H\right)$。相应

地，$\left|\frac{\beta^{(l)}}{\beta^{(k)}}\right| \leqslant \exp\left(-\frac{1}{4}\delta H\right)$。现在

$$(\theta^{(k)}-\theta^{(l)})\beta^{(j)}+(\theta^{(j)}-\theta^{(k)})\beta^{(l)}+(\theta^{(l)}-\theta^{(j)})\beta^{(k)}=0,$$

$$\frac{\beta^{(j)}}{\beta^{(k)}}+\frac{\theta^{(l)}-\theta^{(j)}}{\theta^{(k)}-\theta^{(l)}}=\frac{\theta^{(j)}-\theta^{(k)}}{\theta^{(l)}-\theta^{(k)}}\cdot\frac{\beta^{(l)}}{\beta^{(k)}}=\omega,$$

故由 $\beta=\eta_1^{b_1}\eta_2^{b_2}$ 且令

$$\alpha_1=\frac{\eta_1^{(j)}}{\eta_1^{(k)}}, \qquad \alpha_2=\frac{\eta_2^{(j)}}{\eta_2^{(k)}}, \qquad \alpha_3=\frac{\theta^{(l)}-\theta^{(j)}}{\theta^{(k)}-\theta^{(l)}},$$

得出

$$\alpha_1^{b_1}\alpha_2^{b_2}+\alpha_3=\omega。$$

故由 $\omega=\frac{\theta^{(j)}-\theta^{(k)}}{\theta^{(l)}-\theta^{(k)}}\cdot\frac{\beta^{(l)}}{\beta^{(k)}}$ 知

$$|\omega| \leqslant \exp\left(\alpha-\frac{1}{4}\delta H\right), \text{ 即 } |\alpha_1^{b_1}\alpha_2^{b_2}+\alpha_3| \leqslant \exp\left(\alpha-\frac{1}{4}\delta H\right)。$$

由 $\alpha_1^{b_1}\alpha_2^{b_2}=\omega-\alpha_3$ 得

$$b_1\log|\alpha_1|+b_2\log|\alpha_2|=\log|\omega-\alpha_3|$$

$$=\log|\alpha_3|+\log\left|1-\frac{\omega}{\alpha_3}\right|。$$

因此

$$\left|b_1\log|\alpha_1|+b_2\log|\alpha_2|-\log|\alpha_3|\right|=\left|\log\left|1-\frac{\omega}{\alpha_3}\right|\right|,$$

而

$$\left|\log\left|1-\frac{\omega}{\alpha_3}\right|\right|=\left|\frac{\omega}{\alpha_3}+\frac{1}{2}\frac{\omega^2}{\alpha_3^2}+\cdots\right| \leqslant \left|\frac{\omega}{\alpha_3}\right|\cdot\frac{1}{1-\left|\frac{\omega}{\alpha_3}\right|}。$$

由于 $\left|\frac{\omega}{\alpha_3}\right| \leqslant \exp\left(\alpha-\frac{1}{4}\delta H\right)$，故在 $H \geqslant 6$ 时我们有 $\left|\frac{\omega}{\alpha_3}\right|$

$\leqslant 0.2$ 且

$$\left|\log\left|1-\frac{\omega}{\alpha_3}\right|\right|\leqslant 1.25\left|\frac{\omega}{\alpha_3}\right|\leqslant 6\exp\left(-\frac{1}{4}\delta H\right)。$$

这样，我们就得出：如果$H\geqslant 20$，则

$$|b_1\log|\alpha_1|+b_2\log|\alpha_2|-\log|\alpha_3||\leqslant\exp(-0.404H)。\tag{12}$$

为了利用Baker的定理（见第三章§4的Ⅱ），我们需要确定$\alpha_1,\alpha_2,\alpha_3$的高。$\alpha_1,\alpha_2$和$\alpha_3$分别满足方程

$$x^6-132x^5-4773x^4-27236x^3-4773x^2-132x+1=0,$$

$$x^6+30x^5-783x^4-2408x^3-783x^2+30x+1=0,$$

$$21x^6+63x^5-198x^4-484x^3-198x^2+63x+21=0。$$

故由Baker定理得，(12)中的所有整数解满足

$$\max\{|b_1|,|b_2|\}\leqslant\{4^9(0.404\cdots)^{-1}6^8\log 27236\}^{49}$$

$$\leqslant 10^{563}。\tag{13}$$

由(13)式及$x-y\theta=\pm\eta_1^{b_1}\eta_2^{b_2}$知，可以定出$\max\{|x|,|y|\}$的上界。但这个界太大了，为了证明 4)，我们给出一个引理。

引理 设θ,β是给定的实数，$M,B>6$是给定的整数。再设p,q是整数满足$1\leqslant q\leqslant BM$，$|\theta q-p|\leqslant 2(BM)^{-1}$。则在$\|q\beta\|\geqslant 3B^{-1}$，且$|b_1\theta+b_2-\beta|\leqslant K^{-|b_1|}$时，必有$|b_1|\leqslant\frac{\log(B^2M)}{\log K}\leqslant M$，这里$\|*\|$表示*与最近整数的距离。

证 $|b_1q\theta+b_2q-\beta q|\leqslant qK^{-|b_1|}\leqslant BMK^{-|b_1|}$，并且如果$q\theta=p+\omega$，这里$|\omega|\leqslant 2(MB)^{-1}$，则有

$$|b_1(p+\omega)+b_2q-\beta q|\leqslant BMK^{-|b_1|}。$$

再由$\|\beta q\|\geqslant 3B^{-1}$，$|b_1\omega|\leqslant 2B^{-1}$知，$\|b_1\omega-\beta q\|\geqslant B^{-1}$。因此

$$B^{-1} \leqslant BMK^{-|b_1|},$$

此给出

$$|b_1| \leqslant \frac{\log(B^2M)}{\log K}。$$

证毕。

在引理中，令

$\theta = \dfrac{\log|\alpha_1|}{\log|\alpha_2|}$， $\beta = \dfrac{\log|\alpha_3|}{\log|\alpha_2|}$， $K = e^{0.404}$， $M = 10^{563}$，

$B = 10^{33}$。

则

$$\left| b_1 \frac{\log|\alpha_1|}{\log|\alpha_2|} + b_2 - \frac{\log|\alpha_3|}{\log|\alpha_2|} \right| < 6\exp(-0.543H)。$$

我们计算θ, β的有理逼近。设 θ 的有理逼近是$\dfrac{a}{b}$，满足 $|\theta - \dfrac{a}{b}| < \dfrac{1}{(MB)^2}$，且设$\dfrac{a}{b}$的有理逼近是$\dfrac{p}{q}$，满足 $1 \leqslant q \leqslant MB$，$\left| \dfrac{a}{b} - \dfrac{p}{q} \right| < \dfrac{1}{MB}$。则$\dfrac{p}{q}$是$\theta$的一个有理逼近，满足

$$1 \leqslant q \leqslant MB; \quad |\theta - \frac{p}{q}| < \frac{2}{MBq}。$$

求$\dfrac{a}{b}$和$\dfrac{c}{d}$使得

$$|\theta - \frac{a}{b}| < 10^{-1236}, \quad |\beta - \frac{c}{d}| < 10^{-650}。$$

则对所有情形，$\|q\dfrac{c}{d}\| \geqslant 3 \times 10^{-33}$，故(12)的所有解均满足

$$|b_1| \leqslant \frac{\log 10^{629}}{0.404} \leqslant 3585。$$

在引理中，再取$M = 4500$，$B = 10^2$，易知

$$|b_1| \leqslant \frac{\log(4.5 \times 10)}{0.404} \leqslant 44。$$

这样一来，可以通过$x - y\theta = \pm \eta_1^{b_1} \eta_2^{b_2}$经过计算求出$b_1 = 0$，$b_2 = 0$和$b_1 = 0$，$b_2 = -1$，给出方程$x^3 - 12xy^2 - 12y^3 = 1$仅有解$(1,0)$和$(1,-1)$。

对于$D < 0$，Delaunay[38]和Nagell[39]有过一些研究，例如证明了

定理 3 设 $f(x, y)$ 是判别式为D的给定的二元三次型，$D<0$，则方程$f(x,y) = 1$除 $x^3 + xy^2 + y^3 = 1$（或$x^3 - x^2y + xy^2 + y^3 = 1$）存在 4 组解和$x^3 - xy^2 + y^3 = 1$存在5组解外，最多有 3 组整数解。

由于$D<0$时，三次域$Q(\theta)$（这里θ是$f(\theta,1) = 0$的根）仅有一个基本单位数，故方程$f(x,y) = 1$化为

$$x - y\theta = \eta^m, \quad m \in Z,$$

这里η是基本单位数。由于存在正整数a使得$\eta^a \equiv 1 (\mathrm{mod}\, p)$，这里$p$是任给的素数。故对$m$进行模$a$分类讨论，可得出方程$f(x,y) = 1$的全部解（参阅$p$-adic方法）。

§4 三元三次丢番图方程

现在讨论三元三次丢番图方程的解。

I．丢番图方程$x^3 + y^3 + z^3 = n$

对于丢番图方程

$$x^3 + y^3 + z^3 = n, \quad n \in Z, \tag{1}$$

在 $n=0$ 时化为著名的 Fermat 大定理（参看第八章）的特例。我们来证明

定理 1 丢番图方程 $x^3+y^3+z^3=0$ 无 $xyz\neq 0$ 的整数解。

证 设 x,y,z 是方程 $x^3+y^3+z^3=0$ 的一组解，$xyz\neq 0$，不妨设 $(x,y)=(x,z)=(y,z)=1$，$2\nmid xy$，$2|z$，且 $|z|$ 是 $xyz\neq 0$ 的解中最小的。可设

$$x+y=2a,\quad x-y=2b,\quad (a,\ b)=1,\quad a\neq b,$$

由此解出 x,y，代入方程 $x^3+y^3+z^3=0$ 得

$$-z^3=(a+b)^3+(a-b)^3=2a(a^2+3b^2)。\qquad (2)$$

由 $2\nmid x$ 知 $2\nmid a+b$，故 $2\nmid a^2+3b^2$，故由 $2|z$ 知，(2) 给出 $4|a$，$2\nmid b$。又 $(2a,\ a^2+3b^2)=(a,\ 3)=1$ 或 3，故在 $(2a,a^2+3b^2)=1$ 时，(2) 给出

$$2a=r^3,a^2+3b^2=s^3,\quad -z=rs,\quad 2\nmid s。$$

由 $a^2+3b^2=s^3$ 在 $Q(\sqrt{-3})$ 中讨论立得

$$a=u(u^2-9v^2),\quad b=3v(u^2-v^2),\quad s=u^2+3v^2,$$

这里 $(u,v)=1$，$2|u$，$2\nmid v$，且 $u\neq 0$。由于此时 $3\nmid a$，故 $3\nmid u$，于是 $2u$，$u-3v$，$u+3v$ 两两互素。现在

$$r^3=2a=2u(u-3v)(u+3v),$$

故得

$$2u=-l^3,\quad u-3v=m^3,\quad u+3v=n^3,$$

此给出 $l^3+m^3+n^3=0$，且有 $2|l$，$lmn\neq 0$。但是

$$|z|^3=|2a(a^2+3b^2)|=|l^3(u^2-9v^2)(a^2+3b^2)|$$
$$\geqslant|a^2+3b^2|\ |l^3|>|l|^3,$$

与 $|z|$ 的最小性矛盾。

现设 $(2a,a^2+3b^2)=3$。令 $a=3c$，则 $4|c$，$3\nmid b$。由 (2) 式得

$$-z^3=6c(9c^2+3b^2)=18c(3c^2+b^2),$$

由$(18c,3c^2+b^2)=1$知，上式给出

$$18c=r^3,\quad 3c^2+b^2=s^3。$$

由后一式得出

$$b=u(u^2-9v^2),\quad c=3v(u^2-v^2),\quad s=u^2+3v^2,$$

这里$(u,v)=1$，$2\nmid u$，$2\mid v$，$v\neq 0$。易知 $2v$，$u-v$，$u+v$ 两两互素，故由$r^3=18c$，$c=3v(u^2-v^2)$知

$$\left(\frac{r}{3}\right)^3=2v(u-v)(u+v),$$

推出

$$2v=-l^3,\quad u-v=-m^3,\quad u+v=n^3,\quad lmn\neq 0,$$

由此知$l^3+m^3+n^3=0$，这里$2\mid l$。但是

$$\begin{aligned}|z^3| &= |18c(3c^2+b^2)| = 27|2v(u^2-v^2)|(3c^2+b^2)\\ &= 27|l|^3\cdot|u^2-v^2|(3c^2+b^2)>|l|^3,\end{aligned}$$

仍与$|z|$的最小性矛盾。证毕。

下面讨论方程(1)可设$n\neq 0$。又由于$n<0$时方程(1)化为

$$(-x)^3+(-y)^3+(-z)^3=-n>0,$$

故不妨假设(1)中的 $n>0$。我们在第二章的§1中给出了 $n\equiv\pm 4 \pmod 9$时方程(1)无解的证明。现在我们给出

定理 2 当$1\leqslant n\leqslant 2$时方程(1)有无穷多组解。

证 当$n=1$时，方程(1)化为

$$x^3+y^3+z^3=1。\tag{3}$$

容易验证$x=t$，$y=-t$，$z=1$ 或 $x=9t^4$，$y=3t-9t^4$，$z=1-9t^3$ $(t\in Z)$都是方程(3)的解。当$n=2$时，方程(1)化为

$$x^3+y^3+z^3=2。\tag{4}$$

可以验证 $x=1+6t^3$，$y=1-6t^3$，$z=-6t^2$ $(t\in Z)$ 是(4)的解。证毕。

能否给出(3)和(4)的全部正整数解？在第三章§2的习题1中，我们给出了(4)的解 x, y, z 中至少有一个被6整除，但要给出全部解却不容易。一般的问题是，在$n \not\equiv \pm 4 \pmod 9$时，方程(1)是否都有无穷多组解？

当$n=3$时，已知方程

$$x^3+y^3+z^3=3 \tag{5}$$

有四组解 $(x,y,z)=(1,1,1)$，$(4,4,-5)$，$(4,-5,4)$，$(-5,4,4)$，是否还有其它解？对此Miller和Woolett[40]证明了

定理 3 在$\max(|x|,|y|,|z|)<3164$时，方程(5)除开上述四解外，无其他的整数解。

此外，Miller和Woolett还给出在$\max(|x|,|y|,|z|)<3164$时方程(1)的所有整数解。

1984年，Scarowsky和Boyarsky[41]用大型计算机寻找方程(5)的解。不妨设方程(5)的解满足$x+y+z=3m$，$m\in Z$，则有

定理 4 方程(5)在$|m|<50000$时无其他的解。

1985年，Cassels[42]用环$Z[\omega]$上的三次互反律证明了

定理 5 方程(5)的解满足$x\equiv y\equiv z \pmod 9$。

这个定理我们在第三章的§2中已经证明过了。1987年，孙琦[43]利用三次互反律进一步证明了

定理 6 设a是一个给定的整数，a无$3k+1$形素因子，如果丢番图方程

$$x^3+y^3+z^3=9a^3 \tag{6}$$

有整数解，则9整除$\frac{x}{d}$，$\frac{y}{d}$，$\frac{z}{d}$中的一个，这里$d=(x,y,z)$。

定理 7 设a是一个给定的整数，a无 $3k+1$ 形素因子。如果丢番图方程

$$x^3+y^3+z^3=3a^3 \qquad (7)$$

有整数解，则当 $3\nmid a$ 时有$\frac{x}{d}\equiv\frac{y}{d}\equiv\frac{z}{d}\pmod 9$；而当 $3|a$ 时有

$\frac{x}{d}\equiv\frac{y}{d}\equiv\frac{z}{d}\pmod 9$或9整除$\frac{x}{d}$，$\frac{y}{d}$，$\frac{z}{d}$中的一个，这里 $d=(x,y,z)$。

下面给出定理 6 的证明。设$x=dx_1$，$y=dy_1$，$z=dz_1$代入(6)得

$$d^3(x_1^3+y_1^3+z_1^3)=9a^3。 \qquad (8)$$

设$d=3^\lambda d_1$，$\lambda\geqslant 0$，$3\nmid d_1$，$a=3^t a_1$，$t>0$，$3\nmid a_1$，则(8)给出

$$x_1^3+y_1^3+z_1^3=3^{3(t-\lambda)+2}a_2^3,\quad t\geqslant\lambda, \qquad (9)$$

这里$a_1=d_1a_2$。对(9)取模9知x_1,y_1,z_1中有一被3除尽。不妨设 $x_1\equiv 0\pmod 3$，$y_1\equiv 1\pmod 3$，$z_1\equiv -1\pmod 3$。在整环 $Z[\omega]$中，这里$\omega=\frac{-1+\sqrt{-3}}{2}$，有

$$z_1^3+x_1^3=(z_1+x_1)(z_1+x_1\omega)(z_1+x_1\omega^2),$$

设$\alpha=z_1+x_1\omega$，则$\alpha\equiv 2\pmod 3$，故α可分解为

$$\alpha=\pm\pi_1\cdots\pi_k,$$

其中$\pi_j(j=1,\cdots,k)$是$Z[\omega]$中的本原素数，即$\pi_j\equiv 2\pmod 3$ $(j=1,\cdots,k)$。现对(9)取模$\pi_j(j=1,\cdots,k)$得

$$y_1^3\equiv 3^{3(t-\lambda)+2}a_2^3\pmod{\pi_j},\ j=1,\cdots,k。 \qquad (10)$$

不妨设$\pi_j(j=1,\cdots,k)$均为 $Z[\omega]$ 中的复素数，则$N(\pi_j)=p_j\equiv 1\pmod 3$ $(j=1,\cdots,k)$。由a_2不含 $3k+1$ 形素因子知，$\pi_j\nmid 3a_2(j=1,\cdots,k)$，于是(10)式给出

$$1=\left(\frac{3^2}{\pi_j}\right)_3=\left(\frac{\omega^4(1-\omega)^4}{\pi_j}\right)_3=\left(\frac{\omega}{\pi_j}\right)_3\left(\frac{1-\omega}{\pi_j}\right)_3$$

$$(j=1,\cdots,k)。\qquad (11)$$

设$\pi_j=a_j+b_j\omega$，$b_j=3n_j$，$a_j=3m_j-1$，m_j，$n_j\in Z$（$j=1,\cdots,k$），则有$\left(\frac{\omega}{\pi_j}\right)_3=\omega^{m_j+n_j}$，$\left(\frac{1-\omega}{\pi_j}\right)_3=\omega^{2m_j}$（见第三章§2），故由(11)式知

$$1=\omega^{m_j+n_j}\cdot\omega^{2m_j}=\omega^{n_j}\quad(j=1,\cdots,k),$$

此给出 $n_j\equiv 0(\mathrm{mod}3)$（$j=1,\cdots,k$）。于是 $\alpha=z_1+x_1\omega\equiv u$ $(\mathrm{mod}9)$，$u\in Z$，此给出$9|x_1$，即$9\left|\frac{x}{d}\right.$。证毕。

关于方程（1），要给出全部解是相当困难的。有些简单的方程是否有解也解决不了。例如丢番图方程

$$x^3+y^3+z^3=30$$

有整数解吗？这是一个尚未解决的问题。

Ⅱ. 丢番图方程　$ax^3+by^3+cz^3=d$

现在我们考虑较为一般的丢番图方程

$$ax^3+by^3+cz^3=d。\qquad (12)$$

Segre[44]证明了

定理 8　设a,b,c,d是整数，且$abcd\neq 0$，则方程(12)一般没有解x,y,z是关于参数t的次数$\leqslant 4$的有理系数的互素多项式。

三个不同的例外是，方程

$$x^3+y^3+cz^3=c,$$

$$x^3+y^3+cz^3=2,$$

$$x^3+y^3+2z^3=2,$$

这里$c\neq 2r^3$，r是有理数，它们分别有解：

$x=t, y=-t, z=1$ 和

$$x=-\frac{9}{c}t^4+3t,\quad y=\frac{9}{c}t^4,\qquad z=-\frac{9}{c}t^3+1;$$

$$x=-\frac{6}{c}t^3+1,\quad y=\frac{6}{c}t^3+1,\quad z=-\frac{6}{c}t^2;$$

$x=-4t^2+6t+1$, $y=-4t^2+2t+1$, $z=4t^2-4t+1$ 和

$27x=2(-4t^4+4t^3+6t^2-17t+2)$,

$27y=4(-2t^4+8t^3-6t^2-4t+13)$,

$27z=8t^4-20t^3+24t^2+16t-37$。

利用Gauss关于二次丢番图方程的结果（见第五章§4），可以证明

定理 9 丢番图方程

$$ax^3+ay^3+bz^3=bc^3,\quad abc\neq 0 \tag{13}$$

除了有平凡解$x+y=0$, $z=c$外，还有无穷多组整数解。

证 设$z=c+t(x+y)$，代入(13)式得

$(x+y)[a(x^2-xy+y^2)+3bc^2t+3bct^2(x+y)+bt^3(x+y)^2]=0$,

由于$x+y=0$时(13)给出$z=c$。故除去$x+y=0$, $z=c$, 上式给出

$$a(x^2-xy+y^2)+3bc^2t+3bct^2(x+y)+bt^3(x+y)^2=0。\tag{14}$$

令

$$x+y=u,\quad x-y=v, \tag{15}$$

则 (14) 化为

$$\frac{a}{4}(u^2+3v^2)+3bc^2t+3bct^2u+bt^3u^2=0,$$

由此即得

$$(a+4bt^3)u^2+(3a)v^2+(12bct^2)u+12bc^2t=0。\quad (16)$$

(16)式是Gauss二次丢番图方程的特例（参阅第五章§4）。设$t=-abk^2$，$k\neq 0$，则(16)显然有解$u=0$，$v=2bck$。而在$k\neq 0$时

$$D=-12a(a+4bt^3)=12a^2(4a^2b^4k^6-1)>0,$$

且存在k(如$3|k$)使D非平方数。又

$$\Delta=4(a+4bt^3)3a\cdot 12bc^2t-3a(12bct^2)^2$$
$$=144abc^2t(a+bt^3),$$

由$t=-abk^2$，$k\neq 0$知$t\neq 0$，且可取k使$a+bt^3\neq 0$，故存在k使$\Delta\neq 0$。于是知存在k使(16)有无穷多组解u,v满足$u\equiv v \pmod 2$，这样由(15)式及$z=c+t(x+y)$知(13)有无穷多组解x,y,z。为此，设$2^\alpha \| a$，且可取k使$2^{\alpha+1}|t$，故对(16)取模$2^{\alpha+1}$得

$$au^2+3av^2\equiv 0 \pmod{2^{\alpha+1}},$$

由$2^\alpha\|a$知$u^2+3v^2\equiv 0 \pmod 2$，故$u\equiv v \pmod 2$。证毕。

方程(13)的一个特殊情形是方程(3)(称为Euler方程)，即

$$x^3+y^3+z^3=1,$$

利用定理 9 的证明方法可以构造它的无穷多组解。例如令$z=1+t(x+y)$，$x+y=u$，$x-y=v$，则有

$$(1+4t^3)u^2+3v^2+(12t^2)u+(12t)=0。\quad (17)$$

由于$t|u^2+3v^2$，故可设$t=\pm(\xi^2+3\eta^2)$。如取$t=-7$，则(17)化为

$$-1391u^2+3v^2+588u-84=0,$$

由此整理成

$$(457u-98)^2-457v^2=3192, \quad (18)$$

此显然有解$u=1$，$v=17$，给出(3)有解$(x,y,z)=(9,-8,$

-6)。由(18)的无穷多组解u,v(显然$u\equiv v\pmod 2$)，可得出(3)的无穷多组解。例如（-103，94，64)，(904，-823，-566)，(3097，-2820，-1938)等等。

对于方程(12)的又一类型

$$x^3-my^3=nz^3, \tag{19}$$

如$|m|=1$，则根据n的不同，可以用分解因子法或在域$Q(\omega)\left(\omega=\frac{-1+\sqrt{-3}}{2}\right)$中考虑方程（19）的解。如果$|m|\neq 1$，则在三次域$Q(\theta)$中考虑方程(19)，这里$\theta=\sqrt[3]{m}$，化为理想数方程

$$[x-y\theta]=\eta A^3,$$

这里η是取某有限集的理想。于是有

$$x-y\theta=\mu\alpha^3=(e+f\theta+g\theta^2)(u+v\theta+w\theta^2)^3,$$

这里u,v,w是有理整数，且e,f,g是属于有理数的某个有理子集。乘开后，比较两端θ^2的系数，可以求解形如(19)的丢番图方程。

对于方程(12)中$d=0$的特殊情形

$$ax^3+by^3+cz^3=0, \tag{20}$$

我们有

定理10 如果 $a=\frac{1}{2}p(p+q)(q-2p), b=\frac{1}{2}q(7p+q)\cdot(7p+2q)$，$c=2$或4，$p+q\not\equiv 0\pmod 3$，且

1) $p\equiv 1\pmod 2$，$q(q-p)\equiv 0\pmod 4$或

2) $p\equiv 2\pmod 4$，$q\equiv 1\pmod 2$中的一个，以及 $q^2-qp+7p^2\not\equiv 0\pmod{p_2}$ 或 $pq(63p^2-34pq+9q^2)\not\equiv 0\pmod{p_2}$，这里 $p_2\equiv 1\pmod 3$ 是素数且$\left(\frac{2}{p_2}\right)_3=-1$。则

方程(20)无解。

例如取$p=q=1$，$p_2=7$，则定理10的条件满足，即$p+q\not\equiv 0 \pmod 3$，$p\equiv 1 \pmod 2$，$q(q-p)\equiv 0 \pmod 4$和$pq(63p^2-34pq+9q^2)\not\equiv 0 \pmod{p_2}$，$p_2\equiv 1 \pmod 3$和$\left(\frac{2}{p_2}\right)_3=-1$。故方程$-x^3+20y^3+cz^3=0$ ($c=2$，4) 无解。

定理11 设d无平方因子，$d\equiv \pm 2, \pm 4 \pmod 9$，三次域$Q(\sqrt[3]{d})$的类数为3。如果$[3]=A^3$，$A$是$Q(\sqrt[3]{d})$的一个理想，但不是主理想，则方程

$$x^3+dy^3=3z^3$$

没有有理解。

这个定理的证明，只要注意$Q(\sqrt[3]{d})$中的整数是$a+b\sqrt[3]{d}+c\sqrt[3]{d^2}$，$a,b,c\in Z$，并且$[3]=A^3$由$[3]=[3,\sqrt[3]{d}\pm 1]^3$或$[3,\sqrt[3]{d}\mp 1]^3$给出就够了。

利用简单同余法还可以得到关于方程(20)的一些结果。

对于方程

$$ax^3+by^3+cz^3=dxyz,\ (x,y,z)=1, \tag{21}$$

研究其整数解是很困难的。1960年，柯召[45]和Cassels[46]分别独立地解决了方程(21)当$a=b=c=d=1$时的特例，即有

定理12 丢番图方程$x^3+y^3+z^3=xyz$没有$xyz\neq 0$的整数解。

Ward[47]还证明了丢番图方程$x^3+y^3+5z^3=5xyz$仅有解$x+y=0$，$z=0$。

Ⅲ．丢番图方程$z^2=f(x,y)$和$z^3=g(x,y)$

设$f(x,y)$是一个有理系数的三次多项式，有一个著名的

猜想是：如果方程

$$z^2=f(x,y) \tag{22}$$

有一组解x,y,z，则必有无穷多组解x,y,z。

这个猜想的一些特殊情形已经证明是成立的。例如有

定理13 设$f(x,y)=p^2+lx+my+ax^3+bx^2y+cxy^2+dy^3$，这里$(l,m)=1$，则方程(22)有无穷多组解$x$，$y,z$。

证 用一个线性变换可不失一般地令$l=1$，$m=0$。如果$p=0$，则(22)给出有无穷多组解为$x=0$，$y=dt^2,z=dt^3$，$t\in Z$。如果$p\neq0$，则令 $x=4p^2X$，$y=2pY$，$z=pZ$，代入(22)得

$$Z^2=1+4X+64ap^4X^3+32bp^3X^2Y+16cp^2XY^2+8dpY^3。\tag{23}$$

再令$Z=1+2X-2X^2$，则$Z^2=1+4X-8X^3+4X^4$，于是(23)给出

$$X^4=(2+16ap^4)X^3+8bp^3X^2Y+4cp^2XY^2+2dpY^3。$$

在这个方程中，令$Y=tX$，$t\in Z$是参数，则有

$$X=(2+16ap^4)+8bp^3t+4cp^2t^2+2dpt^3,$$

这就给出(22)有无穷多组解。证毕。

Mordell[48]推广上述结果，证明了

定理14 设$f(x,y)=p^2+lx+my+ax^2+bxy+cy^2+Ax^3+Bx^2y+Cxy^2+Dy^3$，$p\neq0$。如果 $p\mid(l,m)$，且方程

$$ax^2+bxy+cy^2-\left(\frac{lx+my}{2p}\right)^2=\pm2p \tag{24}$$

有无穷多组解，则方程(22)有无穷多组解。

由于（24）是一个二元二次丢番图方程，故一般说来在(24)有解时可得出无穷多组解。Mordell还得到

定理15 设$f(x,y)=(6l^2+6l-1)x^3+(6l^2-6l-1)y^3+11-12l^2$，这里$l\neq 0\in Z$，则方程(22)有无穷多组解。

利用 Pell 方程的结果，可以构造出许多三次多项式$f(x,y)$，使方程(22)有无穷多组解。例如$f(x,y)=x^3+y^3-1$，令$x=1+w$，$y=1-w$，则方程(22)推出

$$z^2-6w^2=1,$$

而这个方程是Pell方程，已知它有无穷多组解z，w。

定理16 设$f(x,y)=ab^2x^3+y^3+(27abd)^2$，$ab\neq 0$，$a,b,d$均是整数，则方程(22)有无穷多组解。

证 考虑方程

$$z^2-k^2=ab(x^3+cy^3),\ ab\neq 0, \tag{25}$$

令$t^3=c$的三个根为$\theta=\theta_1$，θ_2，θ_3，且设

$$z+k=a\prod_{\theta}(p+q\theta+r\theta^2), \tag{26}$$

$$z-k=b\prod_{\theta}(p_1+q_1\theta+r_1\theta^2), \tag{27}$$

这里p,p_1,q,q_1,r和r_1都是整数，则有

$$z^2-k^2=ab\prod_{\theta}(P+Q\theta+R\theta^2)=ab(P^3+bQ^3+b^2R^3-3bPQR),$$

令$P=x$，$Q=y$，$R=0$，即有

$$pp_1+c(qr_1+q_1r)=x, \tag{28}$$

$$pq_1+p_1q+crr_1=y, \tag{29}$$

$$pr_1+p_1r+qq_1=0。 \tag{30}$$

又，由(26)、(27)得

$$2k=a(p^3+cq^3+c^2r^3-3cpqr)-b(p_1^3+cq_1^3+c^2r_1^3-3cp_1q_1r_1)。 \tag{31}$$

令$p_1=q$，$q_1=-r$，$r_1=0$，则(30)成立，且由(28)、(29)和(31)得

$$x=pq-cr^2,\quad y=-pr+q^2,\quad z-k=b(q^3-cr^3),\tag{32}$$

$$2k=a(p^3+cq^3+c^2r^3-3cpqr)-b(q^3-cr^3)。\tag{33}$$

现在令 $c=\frac{b}{a}$，则(33)和(25)分别为

$$2k=ap^3+\frac{2b^2r^3}{a}-3bpqr,\tag{34}$$

$$z^2-k^2=abx^3+b^2y^3。\tag{35}$$

令$k=27ab^2d$，且由bx,bz代x,z，则(35)给出

$$z^2=ab^2x^3+y^3+(27abd)^2。$$

为了证明我们的结论，只要证明有无穷多组解p，q，r 满足(34) 即可。此时令 $p=3bX$，$q=Y$，$r=3aZ$，注意 $k=27ab^2d$，(34)给出

$$2d=bX^3+2aZ^3-XYZ。$$

容易知道，这个方程有无穷多组解。证毕。

这种类型的两个简单方程是

$$z^2=x^3+y^3,\ (x,y)=1,\tag{36}$$

和

$$2z^2=x^3+y^3,\ (x,y)=1。\tag{37}$$

(36)有无穷多组解，如

$$x=-4p^3q+4q^4,\quad y=p^4+8pq^3。$$

Rodeja[49]彻底解决了方程(37)。Georgikopoulous[50]给出了方程

$$z^2=x^3+4y^3,\ (x,y)=(y,z)=(z,x)=1$$

的全部整数解，它们都包含在

$$x=p(p^3+q^3),\quad y=q(q^3-2p^3),$$

$$\pm z = p^6 - 10p^3q^3 - 2q^6$$

中。

另一个类似的问题是：设 $g(x,y)$ 是二次的或三次的多项式，则方程

$$z^3 = g(x,y) \tag{38}$$

是否有无穷多组解（如果有解的话）？一个简单的结果是

定理17 设 $g(x,y)=p^3+lx+my+ax^2+bxy+cy^2$，$(l,m)=1$，则方程(38)有无穷多组解。

这个定理的证明十分容易。例如可设$l=1$，$m=0$，再令$x=3p^2X$，$z=p+X$，$y=tX$即可得。

Euler证明了方程 $x^3+y^3=2z^3$ 仅有 $x=\pm y$的有理解（或整数解），利用这个结果也可证明$3y^2=x^3-1$仅有$y=0$的整数解。

Ⅳ. 其他的一些三元三次丢番图方程

1952年，Mordell[52]考虑了丢番图方程

$$ax^3+by^3+c=xyz \tag{39}$$

的可解性，这里a,b,c均是整数。他证明了

定理18 方程(39)有无穷多组解x,y满足$(x,y)=1$。

利用一些相关序列的性质，还可证明

定理19 丢番图方程$x^2+y^2-x-y+1=xyz$，$x>0$，$y>0$仅有解$x=y=1$。

定理20 丢番图方程

$$x^3+y+1=xyz \tag{40}$$

仅有正整数解 $(x,y,z)=(3,14,1)$，$(2,9,1)$，$(2,3,2)$，$(5,14,2)$，$(1,2,2)$，$(1,1,3)$，$(5,9,3)$，$(3,2,5)$和$(2,1,5)$。但方程(40)却有无穷多组整数解。

定理20是 Mohanty[53] 于1977年才得到的，他同时还

证明了丢番图方程

$$x^3 + y^2 - y + 1 = xyz \tag{41}$$

有无穷多组正整数解。

求出方程(40)的全部正整数解是容易的。首先，我们指出，求解方程(40)与解$x | y+1$且$y | x^3+1$是等价的。因为由(40)易知$x | y+1$且$y | x^3+1$。反过来有$xy | (x^3+1)(y+1)$，推出$xy | x^3+y+1$，故有整数z存在使得$x^3+y+1=xyz$。这样，我们可设

$$y+1=xr,\quad x^3+1=sy,\quad r>0,\quad s>0,$$

由此知

$$s(rx-1)=x^3+1,$$

故有$x(sr-x^2)=s+1$。设$sr-x^2=n$，则$xn=s+1$。我们有

$$x^2=sr-n=r(xn-1)-n=rxn-(n+r)。$$

由此知$rn>x$，可设$rn=x+k$，$k>0$，这时上式给出$xk=r+n$。从$rn=x+k$和$xk=r+n$我们得到

$$(n-1)(r-1)+(x-1)(k-1)=2。\tag{42}$$

由于(42)的左端每一项均是非负的，故有三种情形：

$$(n-1)(r-1)=0,\quad (x-1)(k-1)=2,\tag{43}$$

$$(n-1)(r-1)=2,\quad (x-1)(k-1)=0,\tag{44}$$

$$(n-1)(r-1)=1,\quad (x-1)(k-1)=1,\tag{45}$$

从(43)式知，方程(40)仅有正整数解$(x,y)=(2,1),(2,9),(3,2)$和$(3,14)$。由(44)式得出$(x,y)=(1,1),(1,2),(5,9)$和$(5,14)$。由(45)得出$(x,y)=(2,3)$。因此(40)的全部正整数解为$(x,y)=(3,2),(3,14),(2,1),(2,9),(1,1),(1,2),(5,9),(5,14)$和$(2,3)$。相应的$z=\dfrac{x^3+y+1}{xy}$是5,1,5,

1,3,2,3,2和2。此外，方程(40)显然有无穷多组整数解，例如$(x,y,z)=(0,-1,2),(-1,0,2),(x,-(x^3+1),0),(x,-1,-x^2)$，$(-1,y,-1)$，$(x,-(x^2-x+1),-1)$，$(x,-(x+1),1-x),(-r^2,r^3-1,r)(x,r\in Z)$等等。

这种类型的丢番图方程，我们通过所谓的序列链的讨论，容易给出它们的无穷多组解。一个正整数序列$\{u_i\}$的最小三项是满足 $u_{n-1}u_{n+1}=u_n^3+1$ 的任给的常数项。则由$u_{n-1}u_{n+1}=u_n^3+1$定义的正整数序列$\{u_i\}$称为序列链。

(a) 如果对某些i，$u_i=u_{i+1}$，则有序列链：

$$\cdots,\ 9,2,1,1,2,9,\ \cdots$$

(b) 如果对某些i，$u_i=u_{i+2}$，则由$u_i\cdot u_{i+2}=u_{i+1}^3+1$推出$u_i^2=u_{i+1}^3+1$。由丢番图方程 $x^3+1=y^2$（见§2）仅有正整数解$x=2$，$y=3$知，序列链是：$\cdots$,915,14,3,2,3,14,915,$\cdots$。由于容易知道，两个正整数x,y满足$x|y^3+1$且$y|x^3+1$的充要条件是它们是一个序列链的两个常数项。故（a）和(b)给出方程$x^3+y^3+1=xyz$有无穷多组正整数解。

可以证明以上定义的序列链有无穷多个。

我们也可以推广序列链的定义。设 $f(x)$，$g(x)$是两个具有如下形式的整系数多项式：

$$f(x)=x^m+a_1x^{m-1}+a_2x^{m-2}+\cdots+a_2x^2+a_1x+1,$$

$$g(x)=x^n+b_1x^{n-1}+b_2x^{n-2}+\cdots+b_2x^2+b_1x+1。$$

则对任给的正整数x_0,x_1,y_0,y_1满足

$$x_0x_1=f(y_0),\quad y_0y_1=g(x_0),$$

定义一对序列$\{x_n\}$，$\{y_n\}$ ($n=1,2,\cdots$) 满足

$$x_{n-1}x_{n+1}=f(y_n),\quad y_{n-1}y_{n+1}=g(x_n)。$$

Mohanty[53]已经证明，这样的序列对有无限多个。

§5 四元三次丢番图方程

现在我们来研究丢番图方程

$$x^3+y^3+z^3+w^3=n \tag{1}$$

的整数解。

Ⅰ. $n=0$的情形。此时方程(1)即为

$$x^3+y^3+z^3+w^3=0。 \tag{2}$$

由于用两种方法表一个数为两立方数之和的研究，已经给出方程(2)很多解的例子，例如，

$$1729=10^3+9^3=12^3+1^3, 2^3+34^3=15^3+33^3,$$

$$9^3+15^3=2^3+16^3,$$

等等。关于方程(2)的含参数的整数解也有过一些工作，例如[3]，1830年，Baba找到了解 $x=(s^6-4)s, y=-(s^6+8)s$, $z=s^6+6s^3-4$, $w=-s^6+6s^3+4$；1873年，Kroneck找到了解

$$x=6s^3tf+(t\pm s)tr+3(t\mp s)tf^2,$$

$$y=6s^3tf-(t\pm s)tr-3(t\mp s)tf^2,$$

$$z=-6st^3f+(s\pm t)sr+3(s\mp t)sf^2,$$

$$w=-6st^3f-(s\pm t)sr-3(s\mp t)sf^2,$$

这里$r=s^4+s^2t^2+t^4$；1913年，Osborn 又找到了另外的解

$$x=s^2-7st+63t^2,\quad y=8s^2-20st-42t^2,$$

$$z=-9s^2+7st-7t^2,\quad w=6s^2+20st-56t^2。$$

一个古老的问题是，能否给出方程(2)的全部整数解的表达式？这个问题一直没有解决。最近，范绍舲给出了方程(2)的更为一般的解，即

定理 1 丢番图方程(2)有整数解：

$$x=am-bn,\quad y=-(bm+an+bn),$$
$$z=-(dm-cn),\quad w=-(cm+dm+dn),\qquad (3)$$
这里$a,b,c,d\in Z$，且
$$m=(a+2b)(a^2+ab+b^2)-(c-d)(c^2+cd+d^2),$$
$$n=\begin{cases}(a-b)(a^2+ab+b^2)-(c+2d)(c^2+cd+d^2) & \text{当 } m\neq 0\text{时；}\\ k\in Z, & \text{当 } m=0\text{时。}\end{cases}$$

证 仅需验证由(3)给出的表达式确为(2)的解。这是因为如果$m=0$，则有 $n=k$，所以(3)给出 $x=-bk$，$y=-(a+b)k$，$z=ck$，$w=-dk$，而 $m=(a+b)^3+b^3-c^3+d^3=0$，故(3)在$m=0$时是(2)的解。现设$m\neq 0$。由(3)给出
$$x+y=(a-b)m-(a+2b)n,$$
$$z+w=-(c+2d)m+(c-d)n,$$
$$x^2-xy+y^2=(a^2+ab+b^2)(m^2+mn+n^2),$$
$$z^2-zw+w^2=(c^2+cd+d^2)(m^2+mn+n^2)。$$
故有
$$\begin{aligned}x^3+y^3+z^3+w^3&=(x+y)(x^2-xy+y^2)\\&\quad+(z+w)(z^2-zw+w^2)\\&=\{[(a-b)(a^2+ab+b^2)-(c+2d)(c^2+cd+d^2)]m\\&\quad-[(a+2b)(a^2+ab+b^2)-(c-d)(c^2+cd\\&\quad+d^2)]n\}(m^2+mn+n^2)=0,\end{aligned}$$
这里最后一个等号只要把 m，n 代入即得。这就证明(3)是(2)的解。证毕。

不难验证，Baba，Kroneck和Osborn等的参数解均包含在(3)中。例如，Baba的解是(3)当$a=-s^4+2s$，$b=2s^4+2s$，$c=s^3-2$，$d=-2s^3-2$，$m=s^3$ 和 $n=-s^3+2$ 时的

特例（注：这里m和n已约去公因子$9(s^3+1)(s^6+2s^3+4)$）。

利用文[54]中的方法，还可以用已知的方程（2）的有理解来构造全部整数解。例如，由Euler提出，并经 Binet 完善地求方程（2）的全部有理解可按下述方法进行：

首先，求出丢番图方程

$$W^3+3W(X^2+Y^2+Z^2)+6XYZ=0 \qquad (4)$$

的全部有理解。用行列式表达（4）式为

$$\begin{vmatrix} W & 3Z & -3Y \\ -Z & W & 3X \\ Y & -X & W \end{vmatrix}=0,$$

故必有不全为0的整数$a,b,c,(a,b,c)=1$，使

$$Wa+3Zb-3Yc=0,$$
$$-Za+Wb+3Xc=0,$$
$$Ya-Xb+Wc=0。$$

由此联立方程可解出

$$W=-6\rho abc,\quad X=\rho a(a^2+3b^2+3c^2),$$
$$Y=\rho b(a^2+3b^2+9c^2),\quad Z=3\rho c(a^2+b^2+3c^2),$$

此处 ρ为有理数。

令

$$W=\frac{1}{2}(\alpha+\beta+\gamma+\delta),X=\frac{1}{2}(\alpha+\beta-\gamma-\delta),$$
$$Y=\frac{1}{2}(\alpha-\beta+\gamma-\delta),\quad Z=\frac{1}{2}(\alpha-\beta-\gamma+\delta),$$

解出

$$\left.\begin{aligned} \alpha=\frac{1}{2}(W+X+Y+Z),\quad \beta=\frac{1}{2}(W+X-Y-Z),\\ \gamma=\frac{1}{2}(W-X+Y-Z),\quad \delta=\frac{1}{2}(W-X-Y+Z)。\end{aligned}\right\}(5)$$

则由（4）式容易验证

$$\alpha^3+\beta^3+\gamma^3+\delta^3=0。$$

这就有，方程(2)的全部有理解由(5)式表出。现在，我们说明如何从方程（2）的有理解构造整数解。在（5）中，不妨设 $W-X-Y+Z\neq 0$，令

$$\frac{m_1}{n_1}=\frac{W+X+Y+Z}{W-X-Y+Z},\quad \frac{m_2}{n_2}=\frac{W+X-Y-Z}{W-X-Y+Z},$$

$$\frac{m_3}{n_3}=\frac{W-X+Y-Z}{W-X-Y+Z},$$

由W，X，Y，Z的表达式代入有

$$\frac{m_1}{n_1}=\frac{-6abc+a(a^2+3b^2+3c^2)+}{-6abc-a(a^2+3b^2+3c^2)-}$$

$$\to\frac{b(a^2+3b^2+9c^2)+3c(a^2+b^2+3c^2)}{b(a^2+3b^2+9c^2)+3c(a^2+b^2+3c^2)},$$

$$\frac{m_2}{n_2}=\frac{-6abc+a(a^2+3b^2+3c^2)-}{-6abc-a(a^2+3b^2+3c^2)-}$$

$$\to\frac{b(a^2+3b^2+9c^2)-3c(a^2+b^2+3c^2)}{b(a^2+3b^2+9c^2)+3c(a^2+b^2+3c^2)},$$

$$\frac{m_3}{n_3}=\frac{-6abc-a(a^2+3b^2+3c^2)+}{-6abc-a(a^2+3b^2+3c^2)-}$$

$$\to\frac{b(a^2+3b^2+9c^2)-3c(a^2+b^2+3c^2)}{b(a^2+3b^2+9c^2)+3c(a^2+b^2+3c^2)},$$

此处$(a,b,c)=1$，$(m_i,n_i)=1$ $(i=1,2,3)$。于是我们有

定理 2 丢番图方程(2)的全部整数解可表为

$$x=k\frac{m_1}{n_1}[n_1,n_2,n_3],\quad y=k\frac{m_2}{n_2}[n_1,n_2,n_3],$$

$$z=k\frac{m_3}{n_3}[n_1,n_2,n_3],\quad w=k[n_1,n_2,n_3]。$$

其中k是任意整数。

例如取$a=b=c=1$，则$\frac{m_1}{n_1}=\frac{-6+7+13+15}{-6-7-13+15}=\frac{29}{-11}$，$\frac{m_2}{n_2}=\frac{27}{11}$，$\frac{m_3}{n_3}=\frac{15}{11}$，此时$[n_1,n_2,n_3]=11$，故得(2)的整数解 $x=-29k$，$y=27k$，$z=15k$，$w=11k$，$k\in Z$。但是，这种形式的解不是原问题要求的解。

Ⅱ。$n\neq0$。此时不妨设$n>0$。首先我们指出，在 $n\equiv3\pmod6$，$n\equiv\pm1$，±7，$\pm8\pmod{18}$时，方程(1)均有整数解。这是因为

$$6k+3=k^3+(-k+4)^3+(2k-5)^3+(-2k+4)^3,$$

$$18k+1=(3k+30)^3+(-3k-26)^3+(-2k-23)^3+(2k+14)^3,$$

$$18k+7=(k+2)^3+(6k-1)^3+(8k-2)^3+(-9k+2)^3,$$

$$18k+8=(k-5)^3+(-k+14)^3+(3k-30)^3+(-3k+29)^3。$$

历史上，曾经有过这样一个问题：是否对每一个 n，方程(1)均有整数解？在$n\neq\pm4\pmod9$时，这个问题得到了肯定的回答。目前，人们已经证明$n<1000$时，方程(1)均有整数解。利用Gauss 关于二元二次丢番图方程的结果，还可证明：方程(1)有解时，将有无穷多组。例如，Mordell[55]证明了

定理 3 如果方程(1)有一组解 $(x,y,z,w)=(a,b,c,d)$，使得$-(a+b)(c+d)>0$ 不是平方数，且$a\neq b$或$c\neq d$，则方程(1)有无穷多组解。

证 令 $x=a+X$，$y=b-X$，$z=c+Y$，$w=d-Y$，

代入方程(1)得

$$(a+b)X^2+(a^2-b^2)X+(c+d)Y^2+(c^2-d^2)Y=0。\tag{6}$$

方程(6)是一个二元二次丢番图方程，由第五章§4定理1知，在$D=-4(a+b)(c+d)>0$不是平方数，和

$$\begin{aligned}\varDelta &= -(a+b)(c^2-d^2)^2-(c+d)(a^2-b^2)^2\\ &= -(a+b)(c+d)[(c+d)(c-d)^2\\ &\quad +(a+b)(a-b)^2]\neq 0\end{aligned}\tag{7}$$

时，方程(6)有无穷多组解X,Y，从而方程(1)有无穷多组解x,y。现在由$-(a+b)(c+d)>0$不是平方数知$D>0$且不是平方数。下面证明(7)式成立。假设(7)不成立，即有$\varDelta=0$，推出

$$(c+d)(c-d)^2+(a+b)(a-b)^2=0,$$

故有

$$-(a+b)(c+d)(a-b)^2=(c^2-d^2)^2。\tag{8}$$

如果$a\neq b$，则(8)给出$-(a+b)(c+d)$是一平方数，与假设矛盾。故推出$a=b$，且由(8)给出$c=d$，这仍与假设$a\neq b$或$c\neq d$矛盾。这就证明了我们的定理。

由定理3，容易推出$n=1,2,3$时均有无穷多组解。

此外，利用简单同余法还可给出更为一般的丢番图方程

$$ax^3+by^3+cz^3+dw^3=n\tag{9}$$

的解。例如根据$x^3\equiv 0,\ \pm 1 \pmod 9$，$x^3\equiv 0,\ \pm 1 \pmod 7$，对(9)取模9或模7可给出一些结果。

参 考 文 献

[1] Baker, A., Phil. Trans. Roy. Soc., London, 263(1968), 193—208.

[2] Mordell, L.J., Proc. London Math. Soc., (2) 13(1913), 60—80.

[3] Dickson, L. E., History of the Theory of Numbers, Ⅱ, New York, 1952.

[4] Hall, M., J. London Math. Soc., 28(1953), 379—383.

[5] Ellison, W.J., Ellison, F., Pesek, J., Stahland, C.E. and Stall, D.S., J. Number Theory, 4(1972), 107—117.

[6] Steiner, R.P., Math. Comp., 46(1986), 703—714.

[7] Stolarsky, K.B., Algebraic Numbers and Diophantine Approximation, Marcel Dekker, New York, 1974.

[8] Hemer, O., Doctoral Dissertation, Uppsala, 1952.

[9] Ljunggren, W., Acta Arith., 8(1961), 451—465.

[10] Nagell, T., Vid. Akad. Skrifter Oslo, Nr. 7(1930).

[11] London, H. and Finkelstein, L., Notices Amer. Math. Soc., 16(1969), 816.

[12] Lal, M., Jones, M.F. and Blundon, W.J.,

Dept. of Math., Memorial University of Newfoundland, St. Johns, Newfoundland, 1965— and, Math, Comp., 20(1966),322—325.

[13] Watson,G.N.,Messenger Maths.,48(1919), 1—22。

[14] Ljunggren, W., Norsk Mat. Tidsskrift, **34** (1952), 65—72.

[15] 马德刚，四川大学学报（自然科学版），4(1985),107—116。

[16] 徐肇玉、曹珍富，科学通报，7 (1985), 558—559。

[17] Mordell,L.J., Pacific J. Math., 13(1963), 1347—1351.

[18] Avanesov, È. T., Acta Arith., 12(1967), 409—419.

[19] Ljunggren, W., J. London Math. Soc., 3(1971), 385—391.

[20] Mordell, L.J., J. London Math. Soc., 38(1963),454—458.

[21] Nagell, T., Tôhoku Math. J., 24(1924), 48—53.

[22] Nagell, T., Norsk Mat. Forenings skrifter (I), No. 13(1923).

[23] Ljunggren,W., Skr. Norske Vid. Akad. Oslo, I. No.9 (1942),53pp.

[24] Van der Waall and Robert, W., Simon

Stevin, 46(1972/73),39—51.

[25] 柯召、孙琦，四川大学学报（自然科学版），2(1981),1—5。

[26] 柯召、孙琦，中国科学，12(1981)，1453—1457。

[27] 曹珍富、刘培杰，关于丢番图方程 $x^3 \pm 1 = Dy^2$ 山东师大学报（自然）（待发表）。

[28] 柯召、孙琦，四川大学学报（自然科学版），4(1981)，1—5。

[29] Bremner, A. and Morton, P., Math. Comp., 39(1982), 235—238.

[30] Cohn,J.H.E.,J.London Math. Soc.,42 (1967), 750—752.

[31] Bernstein,L., J. London Math. Soc., 3(1971),118—120.

[32] 曹珍富、曹玉书，黑龙江大学学报（自然科学版），1(1983)，47—49。

[33] Ljunggren,W.,Acta Math., 75(1942), 1—21,

[34] Nagell, T.,J. de Math.,4(1925),209—270.

[35] Ljunggren,W., Math. Scand., 1(1953), 297—309.

[36] Baulin, V.I., Tul'sk Gos. Ped. Inst. U'čen. Zap Fiz Mat.Nauk Vyp.,7(1960), 138—170.

[37] Siegel, C.L., Abh. preuss. Akad. Wiss. Phys. Math. kl (1929), Nr 1.

[38] Delaunay, B., Math. Z., 31(1930), 1—26.
[39] Nagell, T., Math. Z., 28(1928), 10—29.
[40] Miller, J.C.P. and Woolett, M.F.C., J. London Math. Soc., 30(1955), 101—110.
[41] Scarowsky, M. and Boyarsky, A., Math. Comp., 42(1984), 235—236.
[42] Cassels, J.W.S., Math. Comp., 44(1985), 265—266.
[43] 孙琦，科学通报，17(1987)，1285—1287。
[44] Segre, B., Mathematicae Notae (Rosario, Argentina), 11(1951), 1—68.
[45] 柯召，四川大学学报（自然科学版），3(1960)，7—18。
[46] Cassels, J.W.S., Acta Arith., 6(1960), 47—51; and Sansone, G. and Cassels, J. W. S., Acta Arith., 7(1962), 187—190.
[47] Ward, M., Duke Math. J., 26(1952), 553—562.
[48] Mordell, L.J., J. London Math. Soc., 17 (1942), 199—203.
[49] Rodeja, F.E.G., Rivista Mat. Hisp. Am. (1953), 4—13, 229—240.
[50] Georgikopoulous, C., Bull. Soc. Math. Grèce., 24(1948), 13—19.
[51] Cassels, J.W.S., Glasgow Math. J., 27 (1985), 11—18.
[52] Mordell, L.J., Acta Math., 88(1952), 77—

83.
[53] Mohanty,S.P.,J. Number Theory,9(1977), 153-159.
[54] 徐肇玉、曹珍富，哈尔滨工业大学学报，数学增刊(1984)，142—150。
[55] Mordell, L.J.,J.London Math, Soc., 11 (1936),208—218; Addendum,12(1937),80; Corrigendum, 32(1957), 383.

第七章　四次丢番图方程

四次丢番图方程一直吸引着人们的注意，这方面的研究已获得大量的成果。直到今天，人们对它的一些基本类型还怀有浓厚的兴趣。但是，即使对于二元四次的丢番图方程，解决它也并不简单。我们在第一章曾提到的Ljunggren 证明方程 $x^2-2y^4=-1$ 仅有两组正整数解 $(x,y)=(1,1)$ 和 $(239,13)$ 就是一个例子，他用了非常复杂且很深刻的方法才给出了这一结论的证明。

对于四次丢番图方程，Ljunggren，Mordell，Cohn，柯召和孙琦以及曹珍富等均有过大量的工作。对各种基本类型，已得出了一系列的结果。本章的目的就是介绍这方面的成果和问题。

§1　丢番图方程 $a^2x^4-Dy^2=1(a=1,2)$

二元四次丢番图方程最基本的问题是：Pell方程解的序列（称为Pell 序列）中是否含有形为 ax^2 的数？一般地，方程

$$x^2-Dy^2=M,\ D>0\ \text{不是平方数},$$

如果有解，则它的解由有限个递推序列给出，那么这些递推序列中含有 ax^2 形的数吗？这个问题的实质是问方程 $a^2x^4-Dy^2=M$ 或 $x^2-Da^2y^4=M$ 是否有解？本节我们讨论一些

特殊的情形。

对于丢番图方程

$$x^4-Dy^2=1,\ D>0\text{且不是平方数,} \tag{1}$$

首先由 Ljunggren[1]于1942年通过研究二次域和四次域的单位数证明了

定理 1 对给定的D,方程(1)最多有两组正整数解。

对于$D=1785$，方程(1)有两组正整数解$x=13$，$y=4$和$x=239$，$y=1352$。

1966年，Ljunggren[2]又解决了$D=p$是一个奇素数的情形，即有

定理 2 设$D=p$是一个奇素数，则方程(1)除开 $p=5$仅有解$x=3$，$y=4$和$p=29$仅有解 $x=99$，$y=1820$ 外，无其他的正整数解。

证 设x，y是方程(1)的正整数解。如果$2\mid x$,则$(x^2-1,\ x^2+1)=1$，故(1)给出

$$x^2\pm1=py_1^2,\quad x^2\mp1=y_2^2,\quad y=y_1y_2,$$

但此由$x^2\mp1=y_2^2$知不可能。现设$2\nmid x$，则(1)给出

$$x^2\pm1=2py_1^2,\quad x^2\mp1=2y_2^2,\quad y=2y_1y_2。 \tag{2}$$

这里$(y_1,\ y_2)=1$。由第五章§5的定理4知，(2)给出

$$x^2+1=2py_1^2,\quad x^2-1=2y_2^2,\quad y=2y_1y_2。 \tag{3}$$

此由前两式得出$x^2=py_1^2+y_2^2$。由(3)易知$2\mid y_2$，$2\nmid x$，故由$x^2-y_2^2=py_1^2$得出

$$x\pm y_2=pu^2,\quad x\mp y_2=v^2,\quad y_1=uv,$$

这就有 $x=\dfrac{pu^2+v^2}{2}$，$y_1=uv$，代入(3)的第一式得出

$$\left(\frac{pu^2-3v^2}{2}\right)^2+1=2v^4,$$

此由 Ljunggren 关于方程 $x^2-2y^4=-1$ 的定理知，仅有 $\frac{pu^2-3v^2}{2}=1$，$v^2=1$和$\frac{pu^2-3v^2}{2}=239$，$v^2=169$。分别给出定理中的$p=5$和$p=29$的情形。证毕。

1966年，Cohn[3]讨论D使方程$X^2-DY^2=-4$有奇数解的情形，但是Cohn遇到了当时无法解决的方程

$$3x^4-2y^2=1。$$

1967年，Cohn[4] 和 Bumby[5] 分别独立地证明了上述方程仅有两组正整数解$x=1$，$y=1$ 和 $x=3$，$y=11$。因此他们证明了

定理 3 设D使得方程 $X^2-DY^2=-4$ 有奇数解，则方程(1)除开 $D=5$，$x=3$，$y=4$ 和 $D=29$，$x=99$，$y=1820$外，无其他的正整数解。

Cohn[6]还进一步证明了

定理 4 设D使 $X^2-DY^2=-4$ 无奇数解，而 $X^2-DY^2=4$有奇数解，则方程(1)除开$D=725$仅有解 $x=99$，$y=364$外，无其他的正整数解。

1975年，柯召和孙琦[7]以及Cohn[8]分别证明了

定理 5 设$D\equiv 3(\mathrm{mod}\,8)$，且Pell方程 $u^2-Dv^2=1$ 的基本解 $\varepsilon=u_0+v_0\sqrt{D}$满足$2|u_0$，则方程 (1) 无正整数解。

定理 6 设D使得方程$u^2-Dv^2=2$或-2之一有解，则方程(1)除开$D=6$ 仅有解$x=7$，$y=20$外，无其他的正整数解。

定理6在第二章§6的例2中给出了一个证明。

1979年，柯召和孙琦[9]又解决了$D=2p$，p 为一个奇素数的情形。但证明中用到了 Ljunggren 关于方程$x^2-2y^4=-1$ 的结果。1983年，他们[10]给出了$D=2p$ 的一个不用

Ljunggren定理的初等证明，即有

定理 7 设 $D=2p$，p 是一个奇素数，则方程(1)除开 $D=6$，$x=7$，$y=20$外，无其他的正整数解。

对于$D=pq$，p,q为不同的奇素数，柯召和孙琦还有大量的工作（参阅[11]～[13]），例如证明了

定理 8 设$D=pq$，p,q是不同的素数，则在

1） $p\equiv 17(\mathrm{mod}\,24)$，$q\equiv 3(\mathrm{mod}\,8)$时，或

2） $p\equiv 5(\mathrm{mod}\,24)$，$q\equiv 23(\mathrm{mod}\,24)$时，或

3） $p\equiv 5(\mathrm{mod}\,24)$，$q\equiv 3(\mathrm{mod}\,8)$，$\left(\frac{p}{q}\right)=1$ 时，方程(1)均无正整数解。

1980年，柯召和孙琦[14] 对D的较为一般的情形进行了研究，证明了如下的四个定理。

定理 9 设$D\not\equiv 7(\mathrm{mod}\,8)$，$D=p_1\cdots p_s$，$s\geqslant 2$，$p_i$ $(i=1,\cdots,s)$是不同的奇素数，则当

1） $p_1\equiv 1(\mathrm{mod}\,4)$，且$2p_1=a^2+b^2$，$a\equiv\pm 3(\mathrm{mod}\,8)$，$b\equiv\pm 3(\mathrm{mod}\,8)$ 或对某个j，$2\leqslant j\leqslant s$，$\left(\frac{p_j}{p_1}\right)=-1$，和

2） $p_i\equiv 7(\mathrm{mod}\,8)$ $(i=2,\cdots,s)$ 或 $p_i\equiv 3(\mathrm{mod}\,8)$ $(i=2,\cdots,s)$ 时，

方程(1)无正整数解。

定理10 设 $D=p_1\cdots p_s$，$s\geqslant 2$，$p_i\equiv 3(\mathrm{mod}\,4)$ $(i=1,\cdots,s)$是不同的奇素数，则方程(1)无正整数解。

定理11 设 $D=2p_1\cdots p_s$，$s\geqslant 2$，p_i $(i=1,\cdots,s)$ 是不同的奇素数，则当

1） $p_1\equiv 1(\mathrm{mod}\,4)$，$p_i\equiv 7(\mathrm{mod}\,8)$ $(i=2,\cdots,s)$，且 $2p_1=a^2+b^2$，$a\equiv\pm 3(\mathrm{mod}\,8)$，$b\equiv\pm 3(\mathrm{mod}\,8)$或对某个$j$，$2\leqslant$

$j \leqslant s$，$\left(\frac{p_i}{p_1}\right) = -1$时，或

2) $p_1 \equiv 5 \pmod 8$，$p_i \equiv 3 \pmod 8$ $(i = 2, \cdots, s)$ 时，或

3) $p_1 \equiv 5 \pmod 8$，$p_i \equiv 7 \pmod 8$ $(i = 2, \cdots, s)$时，

方程(1)均无正整数解。

定理12 设$D = 2p_1 \cdots p_s$，$s \geqslant 2, p_i \equiv 3 \pmod 4$ $(i = 1, \cdots, s)$均是素数，则方程(1)无正整数解。

1981年，曹珍富[15]证明了：在Pell 方程 $X^2 - DY^2 = -1$有整数解时，方程(1)的正整数解x, y不满足

$$x^2 + y\sqrt{D} = \varepsilon^{2m}, \quad m > 0,$$

这里 $\varepsilon = u_0 + v_0\sqrt{D}$ 是Pell方程$u^2 - Dv^2 = 1$的基本解。换句话说，设δ是$X^2 - DY^2 = -1$的基本解，$\bar{\delta}$满足$\delta\bar{\delta} = -1$，则

$$x^2 \neq \frac{\delta^{4m} + \bar{\delta}^{4m}}{2}, \quad m > 0。$$

利用这个结果，我们给出了$D = pq$的几个结果，特别地，我们有[16]：设$D \equiv 0 \pmod 2$或 $D \equiv 13, 17 \pmod{24}$ 且Pell方程$X^2 - DY^2 = -1$有整数解，则方程(1)无正整数解。1983年，曹珍富[16]进一步获得了

定理13 设$D \equiv 1 \pmod 2$，且Pell方程 $u^2 - Dv^2 = 1$ 的基本解$u_0 + v_0\sqrt{D}$ 满足 $r \mid u_0 + 1$，$r \equiv 3 \pmod 4$ 是某个素数，则方程(1)无正整数解。

由定理13立即推出柯召和孙琦的定理 5。例如，在$D \equiv 3 \pmod 8$和$2 \mid u_0$时，由$u_0^2 - Dv_0^2 = 1$得出 $u_0 \equiv 2 \pmod 4$，故$r \mid u_0 + 1 \equiv 3 \pmod 4$。

下面我们给出定理13的另一个推论：

推论 1 设 $D=p_1\cdots p_s$，$s\geqslant 2$，$p_i(i=1,\cdots,s)$是不同的奇素数，则在

1) $p_i\equiv 3(\mathrm{mod}4)(i=1,\cdots,s)$时，或

2) $p_1\equiv 1(\mathrm{mod}4)$，$p_i\equiv 3(\mathrm{mod}4)$ $(i=2,\cdots,s)$，且对某个 j，$2\leqslant j\leqslant s$，$p_j\equiv 7(\mathrm{mod}8)$，$\left(\frac{p_j}{p_1}\right)=-1$时，或

3) $D\not\equiv 7(\mathrm{mod}8)$，$p_1\equiv 1$ $(\mathrm{mod}4)$，$p_i\equiv 3(\mathrm{mod}4)$ $(i=2,\cdots,s)$，且对某个j，$2\leqslant j\leqslant s$，$\left(\frac{p_j}{p_1}\right)=-1$时，

方程(1)均无正整数解。

证 设$u_0+v_0\sqrt{D}$是Pell方程$u^2-Dv^2=1$ 的基本解，则有$u_0{}^2-Dv_0{}^2=1$，于是

$$(u_0-1)(u_0+1)=Dv_0{}^2。\tag{4}$$

如果$2|u_0$，则$(u_0-1,\ u_0+1)=1$，故(4)给出

$$u_0-1=D_1v_1{}^2,\ u_0+1=D_2v_2{}^2,\ v_0=v_1v_2。\tag{5}$$

由定理13知，D_2不能含有$4k+3$型的素因子，故 $D_2=1$ 或 p_1。当$D_2=1$时，(5)给出 $v_2{}^2-Dv_1{}^2=2$，此时由定理6知方程(1)无正整数解。

当$D_2=p_1$时，只需证明条件2)、3) 的情形。首先在条件2)时，(5)给出

$$p_1v_2{}^2-p_2\cdots p_sv_1{}^2=2,$$

此给出对每一个j，$2\leqslant j\leqslant s$，$\left(\frac{p_1}{p_j}\right)=\left(\frac{2}{p_j}\right)$。但由 $p_1\equiv 1$ $(\mathrm{mod}4)$，存在j，$2\leqslant j\leqslant s$，$p_j\equiv 7(\mathrm{mod}8)$ 知$\left(\frac{p_j}{p_1}\right)=$ $\left(\frac{p_1}{p_j}\right)=\left(\frac{2}{p_j}\right)=1$，与假设 $\left(\frac{p_j}{p_1}\right)=-1$矛盾。在条件3)

时，由于$2|u_0$，由定理13知必有$4|u_0$，故对 $u_0^2-Dv_0^2=1$ 取模8知$D\equiv 7 \pmod 8$，与假设$D\not\equiv 7 \pmod 8$矛盾。

如果$2\nmid u_0$，则(4)式给出

$$u_0-1=2D_1v_1^2,\ u_0+1=2D_2v_2^2,\ v_0=2v_1v_2。 \tag{6}$$

这里$v_1>0$，$v_2>0$，且$(v_1, v_2)=1$。由定理13知 $D_2=1$ 或 p_1。当$D_2=1$时，(6)给出$v_2^2-Dv_1^2=1$，但 $v_0=2v_1v_2>v_1>0$与v_0的最小性矛盾。故$D_2=p_1$，此时只要考虑2)、3)的情形。由(6)给出

$$p_1v_2^2-p_2\cdots p_sv_1^2=1, \tag{7}$$

故在存在j，$2\leqslant j\leqslant s$，$\left(\frac{p_j}{p_1}\right)=-1$ 时，上式显然不可能。这就证明了推论。证毕。

因为在(7)有解时，方程(1)给出

$$x^2=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2}=\frac{\Omega^{2n}+\bar{\Omega}^{2n}}{2},\ n>0, \tag{8}$$

这里$\bar{\varepsilon}$满足 $\varepsilon\bar{\varepsilon}=1$，$\Omega=v_2\sqrt{p_1}+v_1\sqrt{p_2\cdots p_s}$，$\Omega\bar{\Omega}=1$。由(8)知

$$x^2+1=\begin{cases} 2p_1\left(\dfrac{\Omega^n+\bar{\Omega}^n}{2\sqrt{p_1}}\right)^2, & 当2\nmid n, \\ 2\left(\dfrac{\Omega^n+\bar{\Omega}^n}{2}\right)^2, & 当2|n。\end{cases}$$

由第五章§5 可知，$2|n$ 时容易处理，而 $2\nmid n$ 时，得出方程 $x^2+1=2p_1y_1^2$。由Lienen定理(见第五章§3)知，在$2p_1=a^2+b^2$，$a\equiv\pm 3 \pmod 8$，$b\equiv\pm 3 \pmod 8$时，方程 $x^2+1=2p_1y_1^2$无解。故可得

推论 2 设$D\not\equiv 7 \pmod 8$，$D=p_1\cdots p_s$，$s\geqslant 2$，$p_i\ (i=1,\cdots, s)$是不同的素数，且$2p_1=a^2+b^2$，$a\equiv\pm 3 \pmod 8$，

$b\equiv\pm3(\bmod 8)$ 和 $p_i\equiv3(\bmod 4)(i=2,\cdots,s)$，则方程(1)无正整数解。

为了证明定理13，我们首先证明一个引理。

引理 设Pell方程$u^2-Dv^2=1$的基本解 $u_0+v_0\sqrt{D}$满足$r\mid u_0+1$，$r\equiv7(\bmod 8)$ 是某个素数，则方程(1)无正整数解。

证 设 $\varepsilon=u_0+v_0\sqrt{D}$，$\bar{\varepsilon}=u_0-v_0\sqrt{D}$，则(1)给出

$$x^2=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2},\ n>0, \tag{9}$$

在 $r\mid u_0+1$，$r\equiv3(\bmod 4)$ 是某个素数时，对(9)式取模r知$2\mid n$。设$n=2n_1$，$n_1>0$，则(9)给出

$$x^2+1=\frac{\varepsilon^{2n_1}+\bar{\varepsilon}^{2n_1}+2(\varepsilon\bar{\varepsilon})^{n_1}}{2}=2\left(\frac{\varepsilon^{n_1}+\bar{\varepsilon}^{n_1}}{2}\right)^2, \tag{10}$$

(10)式是一个Pell方程，解之得

$$\frac{\varepsilon^{n_1}+\bar{\varepsilon}^{n_1}}{2}=\frac{\rho^{2m+1}-\bar{\rho}^{2m+1}}{2\sqrt{2}},\ m\geqslant0, \tag{11}$$

其中 $\rho=1+\sqrt{2}$，$\bar{\rho}=1-\sqrt{2}$，$\rho\bar{\rho}=-1$。由于柯召和孙琦[7]证明了方程

$$x^2=\frac{\varepsilon^{4m}+\bar{\varepsilon}^{4m}}{2},\quad m>0$$

无解，故(11)中的n_1满足$2\nmid n_1$。于是对(11)取模r得

$$\frac{\rho^{2m+1}-\bar{\rho}^{2m+1}}{2\sqrt{2}}=\frac{\varepsilon^{n_1}+\bar{\varepsilon}^{n_1}}{2}\equiv-1(\bmod r)。 \tag{12}$$

由于

$$\frac{\rho^{2m+1}-\bar{\rho}^{2m+1}}{2\sqrt{2}}+1$$

$$=\begin{cases}(\rho^{2m_1}+\bar{\rho}^{2m_1})\left(\frac{\rho^{2m_1+1}-\bar{\rho}^{2m_1+1}}{2\sqrt{2}}\right), & \text{当} m=2m_1,\ m_1\geqslant 0 \text{时；}\\ (\rho^{2m_1+2}+\bar{\rho}^{2m_1+2})\left(\frac{\rho^{2m_1+1}-\bar{\rho}^{2m_1+1}}{2\sqrt{2}}\right), & \text{当} m=2m_1+1,\ m_1\geqslant 0 \text{时。}\end{cases}$$

和 $s^2-2\left(\frac{\rho^{2m_1+1}-\bar{\rho}^{2m_1+1}}{2\sqrt{2}}\right)^2=-1$，故

$r\nmid\frac{\rho^{2m_1+1}-\bar{\rho}^{2m_1+1}}{2\sqrt{2}}$，所以(12)式给出

$$\rho^{2l}+\bar{\rho}^{2l}\equiv 0(\bmod r),\quad l=m_1\text{或}m_1+1。\tag{13}$$

在$r\equiv 7(\bmod 8)$时，$r\nmid 2t^2+1$。但

$$\left(\frac{\rho^{2l}+\bar{\rho}^{2l}}{2}\right)^2-2t^2=1,$$

与(13)式矛盾。这就证明了引理。证毕。

定理13的证明：此时由引理证明知，(13)式之前的证明均成立。于是将(10)式代入(1)得出

$$x^2-1=8Dy_1^2,\quad y=4y_1\left(\frac{\varepsilon^{n_1}+\bar{\varepsilon}^{n_1}}{2}\right),$$

这由前一式又得

$$x\pm 1=4la^2,\ x\mp 1=2kb^2,\ D=lk,\ y_1=ab,\ 2\nmid b,\tag{14}$$

其中$(l,k)=1$，$(a,b)=1$。现由(10)解出x得

$$x=\frac{\rho^{2m+1}+\bar{\rho}^{2m+1}}{2},\ m\geqslant 0,\ \rho=1+\sqrt{2},\ \rho\bar{\rho}=-1。$$

故重复第五章§5的定理 4 的证明（参阅[17]）可知(14)给出

$$k_1^2b_1^4-2l_1^2a_1^4=1,\ k_2^2b_2^4-2l_2^2a_2^4=-1, \tag{15}$$

其中$l=l_1l_2$，$a=a_1a_2$，$k=k_1k_2$，$b=b_1b_2$，且注意到(13)式知$r|k_1b_1^2$，$r\equiv3(\mathrm{mod}\,4)$是某个素数。由(15)的第一式得

$$k_1b_1^2\pm1=4u^2,\ k_1b_1^2\mp1=2v^2,\ 2uv=l_1a_1^2,$$

由$r|k_1b_1^2$及$r\nmid4u^2+1$知，此仅有

$$k_1b_1^2+1=4u^2,\ k_1b_1^2-1=2v^2,\ 2uv=l_1a_1^2,$$

从而

$$v^2-2u^2=-1,\ 2uv=l_1a_1^2。 \tag{16}$$

因为$D\equiv1(\mathrm{mod}\,2)$，$l_1|D$，故$l_1\equiv1(\mathrm{mod}\,2)$。由$2\nmid v$知（16）的后一式给出 $2|u$，但(16)的第一式给出 $2\nmid u$，矛盾。这就证明了我们的定理。证毕。

用类似的方法，曹珍富[16][17]还研究了$D=2p_1\cdots p_s$的情形，证明了

定理14 设$D=2p_1\cdots p_s$，$s\geqslant2$，$p_i(i=1,\cdots,s)$是不同的奇素数，则在

1） $p_1\equiv5(\mathrm{mod}\,8)$，$p_i\equiv3(\mathrm{mod}\,4)(i=2,\cdots,s)$时，或

2） $p_1\equiv1(\mathrm{mod}\,8)$，$p_i\equiv3(\mathrm{mod}\,4)(i=2,\cdots,s)$，且$2p_1=a^2+b^2$，$a\equiv\pm3(\mathrm{mod}\,8)$，$b\equiv\pm3(\mathrm{mod}\,8)$或对某个$j$，$2\leqslant j\leqslant s$，$\left(\frac{p_j}{p_1}\right)=-1$时，

方程(1)除开$D=210$仅有解$x=41$，$y=116$和$D=184030$仅有解$x=47321$，$y=5219916$外，无其他的正整数解。

定理15 设 $D\not\equiv7(\mathrm{mod}\,8)$，$D=p_1\cdots p_s$，$s\geqslant3$，则在

1） $p_1\equiv p_2\equiv1(\mathrm{mod}\,4)$，$p_i\equiv3(\mathrm{mod}\,4)(i=3,\cdots,s)$，$\left(\frac{p_2}{p_1}\right)=-1$ 且存在j，$3\leqslant j\leqslant s$，使$\left(\frac{p_j}{p_1}\right)=-\left(\frac{p_j}{p_2}\right)$时，

或

2) $p_1\equiv p_2\equiv 1(\mathrm{mod}4)$，$p_i\equiv 3(\mathrm{mod}4)$ $(i=3,\cdots,s)$，且存在j，$3\leqslant j\leqslant s$，使$\left(\frac{p_j}{p_1}\right)=-1$，$\left(\frac{p_j}{p_2}\right)=1$ 和 $2p_2=a^2+b^2$，$a\equiv\pm 3(\mathrm{mod}8)$，$b\equiv\pm 3(\mathrm{mod}8)$时，或

3) $p_1\equiv 1(\mathrm{mod}12)$，$p_2\equiv 5(\mathrm{mod}12)$，$p_i\equiv 3(\mathrm{mod}4)$ $(i=3,\cdots,s)$，且$\prod_{i=3}^{s}p_i\not\equiv 1(\mathrm{mod}3)$，和 $2p_1=a^2+b^2$，$a\equiv\pm 3(\mathrm{mod}8)$，$b\equiv\pm 3(\mathrm{mod}\ 8)$或对某个$j$，$2\leqslant j\leqslant s$，$\left(\frac{p_j}{p_1}\right)=-1$时，方程(1)均无正整数解。

1983年，康继鼎、万大庆和周国富[18]以及贾广聚和曹珍富[19]对推论 1 中的3)、推论 2 以及定理 14 也分别给出证明。并且文献[19]的证明中除几个熟知结果外，仅用到分解因子这一初等方法。1983年，曹珍富[16]和康继鼎等[20]还分别独立地证明了

定理16 设$D=2pq$，p，q是不同的奇素数，且$\left(\frac{q}{p}\right)=-1$，则方程(1)无正整数解。

应该指出，柯召和孙琦[13]曾证明：在 $D=2pq$，$p\equiv q\equiv 1(\mathrm{mod}4)$，$\left(\frac{q}{p}\right)=-1$，且$u^2-Dv^2=1$的基本解 $\varepsilon=u_0+v_0\sqrt{D}$满足$r\mid u_0$，$r\equiv 3(\mathrm{mod}4)$是某个素数时，方程(1)无正整数解。曹珍富[15]在1981年曾证明：在 $D=2pq$，$p\equiv q\equiv 5(\mathrm{mod}8)$时，方程(1)无正整数解。

1984年，朱南、罗明和胡世明[21]用递推序列的方法，证明了

定理17 设Pell方程$u^2-Dv^2=1$的基本解 $u_0+v_0\sqrt{D}$ 满足$u_0=4k+3$或$2^{2k+1}(2l+1)$，$k\geqslant 0$，$l\geqslant 0$，则方程(1)无正整数解。

1985年前后，朱卫三[22]和曹珍富[23]分别独立地证明了

定理18 丢番图方程(1)有正整数解的充要条件是存在正整数x_1，y_1使得

$$x_1{}^2+y_1\sqrt{D}=\varepsilon\text{或}\varepsilon^2,$$

这里 $\varepsilon=u_0+v_0\sqrt{D}$是Pell方程$u^2-Dv^2=1$的基本解。

证 充分性显然。下证必要性。设(1)有解，则

$$x_1{}^2+y_1\sqrt{D}=\varepsilon^n,\quad n\geqslant 1 \tag{17}$$

有解。设$n=n_0$为最小解，若$n_0>2$，则可设$n_0=4m$ 或 $n_0=pm$，p 为奇素数，$m\geqslant 1$。在$n_0=4m$时，由柯召和孙琦[7]的一个结果知不可能。而在 $n_0=pm$时，由(17)得出

$$x_1{}^2=\frac{\varepsilon^{pm}+\bar{\varepsilon}^{pm}}{2}=\left(\frac{\varepsilon^m+\bar{\varepsilon}^m}{2}\right)\frac{(\varepsilon^m)^p+(\bar{\varepsilon}^m)^p}{\varepsilon^m+\bar{\varepsilon}^m}。\tag{18}$$

由于$\left(\frac{\varepsilon^m+\bar{\varepsilon}^m}{2},\ \frac{(\varepsilon^m)^p+(\bar{\varepsilon}^m)^p}{\varepsilon^m+\bar{\varepsilon}^m}\right)=1$或$p$，故由(18)式得出

$$\frac{\varepsilon^m+\bar{\varepsilon}^m}{2}=u^2,\qquad \frac{(\varepsilon^m)^p+(\bar{\varepsilon}^m)^p}{\varepsilon^m+\bar{\varepsilon}^m}=v^2,\tag{19}$$

或

$$\frac{\varepsilon^m+\bar{\varepsilon}^m}{2}=pu^2,\qquad \frac{(\varepsilon^m)^p+(\bar{\varepsilon}^m)^p}{\varepsilon^m+\bar{\varepsilon}^m}=pv^2。\tag{20}$$

由$1\leqslant m<n_0$知，(19)的第一式与n_0的最小性矛盾。

现在来证明(20)也不成立。记 $E(p)=\frac{(\varepsilon^m)^p+(\bar{\varepsilon}^m)^p}{\varepsilon^m+\bar{\varepsilon}^m}$，易知 $E(p)\equiv 1\pmod 4$，故 $p\equiv 1\pmod 4$ 利用类似第二章§5的方

法可知对任何奇素数$q \neq p$，均有

$$\left(\frac{E(p)}{E(q)}\right)=1。$$

于是对(20)的第二式取模$E(q)$得出

$$1=\left(\frac{E(p)}{E(q)}\right)=\left(\frac{p}{E(q)}\right)=\left(\frac{E(q)}{p}\right)。\tag{21}$$

记$\varepsilon^m=u_m+v_m\sqrt{D}$，则(20)的第一式给出$p|u_m$，故得

$$E(q)\equiv q(v_m\sqrt{D})^{q-1}=q(u_m^2-1)^{\frac{q-1}{2}}\equiv(-1)^{\frac{q-1}{2}}q(\bmod p),$$

注意到$p\equiv1(\bmod 4)$，由(21)给出

$$1=\left(\frac{E(q)}{p}\right)=\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right)=\left(\frac{q}{p}\right)。$$

由于我们可取q是模p的二次非剩余，故与上式矛盾。这就证明，使(17)式有解的最小$n\leqslant2$，从而证得定理18。证毕。

朱卫三同时指出，在$u_0\geqslant2^{594}$时，方程(1)最多有一组正整数解。虽然定理18给出了方程(1)有正整数解的充要条件，但它不能推出前面的结果。用定理18来证明前面的各个定理，与不用定理18的证明在难度上是相同的。

对于丢番图方程

$$4x^4-Dy^2=1,\ D>0且不是平方数,\tag{22}$$

1982年，曹珍富[24]完全解决了$D=p$是一个奇素数情形，证明了

定理19 设$D=p$是一个素数，则方程(22)除开$p=3$仅有解$x=y=1$和$p=7$仅有解$x=2$，$y=3$外，无其他的正整数解。

证 在$D=p$是一个素数时，由(22)得出

$$2x^2\pm1=py_1^2,\ 2x^2\mp1=y_2^2,\ y=y_1y_2。\tag{23}$$

其中$(y_1,y_2)=1$。由前两式得$4x^2=py_1{}^2+y_2{}^2$，故有

$$2x\pm y_2=pu^2,\ 2x\mp y_2=v^2,\ y_1=uv, \tag{24}$$

这里$(u,v)=1$。由(24)解出 $x=\dfrac{pu^2+v^2}{4}$，$y_1=uv$代入(23)的第一式得

$$p^2u^4+2pu^2v^2+v^4\pm 8=8pu^2v^2,$$

由此整理得

$$2\left(\frac{pu^2-3v^2}{4}\right)^2\pm 1=v^4,$$

显然，上式取“+”时，给出$\dfrac{pu^2-3v^2}{4}=0$，$v^2=1$，给出$p=3$，$x=y=1$，上式取“-”号时，给出$\dfrac{pu^2-3v^2}{4}=\pm 1$，$v^2=1$，故给出$p=7$，$x=2$，$y=3$。证毕。

在这个定理证明中，用到了方程$x^4-2y^2=1$和$x^4+1=2y^2$的两个简单的结果，它们的证明参阅第二章§3（分别作为方程$x^4+y^4=z^2$和$x^4+y^4=2z^2$的推论）。

1985年，曹珍富与曹玉书[25]又研究了 $D=pq$，p,q 是不同的奇素数的情形，证明了

定理20 设$D=pq$，p,q是不同的素数，则在

1） $p\equiv 1(\mathrm{mod}\,8)$，$\left(\dfrac{q}{p}\right)=-1$ 且 $p=a^2+b^2$，$a\equiv 0(\mathrm{mod}\,8)$时，或

2） $p\equiv 1(\mathrm{mod}\,8)$，$q\equiv 7(\mathrm{mod}\,8)$，$\left(\dfrac{q}{p}\right)=1$ 且 $p=a^2+b^2$，$a\equiv 4(\mathrm{mod}\,8)$时，方程(22)均无正整数解。

曹珍富[23]和朱卫三[22]还证明了

定理21 设 $\varepsilon=u_0+v_0\sqrt{D}$是Pell方程$u^2-Dv^2=1$ 的基本解，则方程(22)有解的充要条件是，存在正整数x_1,y_1使得

$$2x_1{}^2+y_1\sqrt{D}=\varepsilon。$$

§2 丢番图方程$x^2-Da^2y^4=1(a=1,\ 2)$

对于丢番图方程

$$x^2-Dy^4=1,\ D>0\text{且不是平方数}, \tag{1}$$

1936年，Ljunggren[26]首先证明了

定理 1 对每一个D，方程(1)最多有两组正整数解。设ε是二次域$Q(\sqrt{D})$的基本单位数，如果方程(1)有两组正整数解，则它们由

$$x+y^2\sqrt{D}=\varepsilon,\ \varepsilon^2 \text{ 或 } x+y^2\sqrt{D}=\varepsilon,\varepsilon^4$$

之一给出，并且后一情形仅对有限个D出现。

1964年，Mordell[27]证明了

定理 2 设$D\neq 0,3,8,15(\mathrm{mod}16)$，且$D$不具有以下任何一种分解：$D=uv,(u,v)=1$，$u>1$是奇数，$u\equiv\pm1(\mathrm{mod}16)$或$u\equiv v\pm1(\mathrm{mod}16)$ 或$u\equiv 4v\pm1(\mathrm{mod}16)$，则方程(1)没有正整数解。

对于 $D=p\equiv1(\mathrm{mod}4)$ 是一个素数，$p\not\equiv1\ (\mathrm{mod}16)$，Mordell证明了方程(1)除开$p=5$仅有解$x=9$，$y=2$外，无其他的正整数解。

1966年，Ljunggren[2]发现$p\not\equiv1(\mathrm{mod}16)$的条件可以去掉，他证明了

定理 3 设$D=p\equiv1(\mathrm{mod}4)$是一个素数，则方程(1)除

开$p=5$仅有解$x=9$，$y=2$外，无其他的正整数解。

证 在$D=p\equiv 1(\bmod 4)$是一个素数时，$N(\varepsilon)=-1$(见第五章§3)，故(1)给出

$$x+y^2\sqrt{p}=\varepsilon^{2n}=(a+b\sqrt{p})^2, \tag{2}$$

式中$a^2-pb^2=(-1)^n$。由(2)得

$$y^2=2ab。 \tag{3}$$

如果$2\nmid n$，则$2\nmid b$，所以(3)式给出

$$a=2h^2,\quad b=k^2,$$

由此知

$$4h^4-pk^4=-1,$$

即

$$(2h^2-2h+1)(2h^2+2h+1)=pk^4。$$

由此即得

$$2h^2\pm 2h+1=pk_1{}^4,\quad 2h^2\mp 2h+1=k_2{}^4,$$

此由$2h^2\mp 2h+1=k_2{}^4$整理得

$$(2h\mp 1)^2+1=2k_2{}^4,$$

由此得出（参阅Ljunggren关于方程 $x^2+1=2y^4$ 的结果）$2h\mp 1=\pm 1$，$k_2=\pm 1$和 $2h\mp 1=\pm 239$，$k_2=\pm 13$，仅给出$p=5$，$x=9$，$y=2$。

如果$2\mid n$，则(2)给出

$$x+y^2\sqrt{p}=(u+v\sqrt{p})^4,$$

从而

$$y^2=4uv(u^2+pv^2),\quad u^2-pv^2=\pm 1。 \tag{4}$$

由(4)推出$u=e^2$，$v=f^2$和 $u^2+pv^2=2u^2\mp 1=g^2$，这就有

$$g^2=2e^4\mp 1。$$

这是两个有熟知结果的方程，把它们的解代入(4)验证知，均不给出方程(1)的正整数解。证毕。

1966年以后，Cohn对方程(1)做了大量的工作。他证明了

定理 4[3] 设D使得方程$X^2-DY^2=-4$有奇数解，则方程（1）除开 $D=5$，$x=9$，$y=2$ 外，无其他的正整数解。

定理 5[6] 设 D 使得方程 $X^2-DY^2=-4$ 没有奇数解，而方程$X^2-DY^2=4$有奇数解，则方程(1)最多有一组正整数解。

对于丢番图方程

$$x^2-4Dy^4=1,\ D>0\text{且不是平方数}, \qquad (5)$$

Cohn 在定理4、5的条件下也得出了相应的结果。1967年，Cohn[28]研究了使Pell方程 $u^2-Dv^2=-1$ 有整数解的方程(1)、(5)的解，证明了

定理 6 设Pell方程$u^2-Dv^2=-1$ 有整数解，且$D\equiv 9,10,13 \pmod{16}$，或 $D\equiv 2 \pmod{16}$，D 有一个因子$\equiv 5 \pmod 8$，则方程(1)和(5)均无正整数解。

实际上，在$u^2-Dv^2=-1$有解且 $D\equiv 0 \pmod 2$时，可证[32]方程(1)无正整数解。

1975年，Cohn[29]对于使得方程$u^2-Dv^2=2\eta(\eta=\pm 1)$有整数解的$D$又研究了方程(1)和(5)的解。

定理 7 设$D>2$使方程$u^2-Dv^2=2\eta(\eta=\pm 1)$ 有整数解，则在$X^4-DY^4=2\eta$，$4X^4-DY^4=2\eta$ 都没有整数解时，方程(1)和(5)也都没有正整数解。

1978年，Cohn[30]进一步给出了$D\leqslant 400$时方程(1)有正整数解的全部D，即 $D=3$，5，8，14，15，18，20，24，33，35，39，48，60，63，65，68，79，80，83，95，99，105，120，138，143，150，156，168，183，189，195，

203, 224, 248, 254, 255, 258, 264, 288, 315, 320, 325, 328, 333, 360, 390和399时，方程(1)有正整数解。

1981 年，柯召和孙琦[31]对D是两个素数乘积的情形，作了详细的探讨。他们证明了

定理 8 设$D=pq$，p,q是素数，则在

1） $p\equiv1\pmod{16}$，$q\equiv7,11\pmod{16}$，$\left(\frac{q}{p}\right)=-1$时，

或

2） $p\equiv9\pmod{16}$，$q\equiv3,15\pmod{16}$，$\left(\frac{q}{p}\right)=-1$时，或

3） $p\equiv5\pmod{16}$，$q\equiv15\pmod{16}$，$\left(\frac{q}{p}\right)=-1$时，或

4） $p\equiv13\pmod{16}$，$q\equiv3,7\pmod{16}$，$\left(\frac{q}{p}\right)=-1$时，或

5） $p\equiv1\pmod{16}$，$q\equiv3,15\pmod{16}$，$\left(\frac{q}{p}\right)=-1$，且

$p=a^2+b^2$，$b\equiv4\pmod8$时，或

6） $p\equiv9\pmod{16}$，$q\equiv7,11\pmod{16}$，$\left(\frac{q}{p}\right)=-1$，且

$p=a^2+b^2$，$b\equiv4\pmod8$时，

方程(1)均无正整数解。

定理8中的1)～4)是以下定理的推论[31]。

定理 9 设$D\equiv7,11\pmod{16}$，且Pell方程$u^2-Dv^2=1$的基本解$\varepsilon=u_0+v_0\sqrt{D}$满足$2|u_0$，则方程(1)无正整数解。

证： 如果$2|x$，则由(1)得出

$$x^2\equiv D+1\pmod{16},$$

此在$D\equiv 7,11 \pmod{16}$时均不成立。于是可设(1)的解满足$2\nmid x$，$2\mid y$。由(1)得出

$$x=\frac{\varepsilon^{n}+\bar{\varepsilon}^{n}}{2},\quad y^{2}=\frac{\varepsilon^{n}-\bar{\varepsilon}^{n}}{2\sqrt{D}},\ n>0, \tag{6}$$

这里$\bar{\varepsilon}=u_0-v_0\sqrt{D}$，$\varepsilon\bar{\varepsilon}=1$。因为$2\mid u_0$，$2\nmid x$，故(6)的第一式给出$2\mid n$。设$n=2m$，$m>0$，由(6)的第二式得

$$y^{2}=\frac{\varepsilon^{2m}-\bar{\varepsilon}^{2m}}{2\sqrt{D}}=2\left(\frac{\varepsilon^{m}+\bar{\varepsilon}^{m}}{2}\right)\left(\frac{\varepsilon^{m}-\bar{\varepsilon}^{m}}{2\sqrt{D}}\right),$$

因为$\left(\frac{\varepsilon^{m}+\bar{\varepsilon}^{m}}{2}\right)^{2}-D\left(\frac{\varepsilon^{m}-\bar{\varepsilon}^{m}}{2\sqrt{D}}\right)^{2}=1$，即

$$\left(\frac{\varepsilon^{m}+\bar{\varepsilon}^{m}}{2},\ \frac{\varepsilon^{m}-\bar{\varepsilon}^{m}}{2\sqrt{D}}\right)=1,\quad \text{故上式给出}$$

$$\frac{\varepsilon^{m}+\bar{\varepsilon}^{m}}{2}=2y_1^{2},\quad \frac{\varepsilon^{m}-\bar{\varepsilon}^{m}}{2\sqrt{D}}=y_2^{2}, \tag{7}$$

或

$$\frac{\varepsilon^{m}+\bar{\varepsilon}^{m}}{2}=y_1^{2},\quad \frac{\varepsilon^{m}-\bar{\varepsilon}^{m}}{2\sqrt{D}}=2y_2^{2}, \tag{8}$$

其中$y=2y_1y_2$。由(7)得出

$$4y_1^{4}-Dy_2^{4}=1。$$

这在$D\equiv 7,11 \pmod{16}$时，显然不成立。由(8)知$2\nmid y_1$，故由$2\mid u_0$推出$2\mid m$。设$m=2h$，$h>0$，则(8)给出

$$\frac{\varepsilon^{2h}+\bar{\varepsilon}^{2h}}{2}=y_1^{2},\ \left(\frac{\varepsilon^{h}+\bar{\varepsilon}^{h}}{2}\right)\left(\frac{\varepsilon^{h}-\bar{\varepsilon}^{h}}{2\sqrt{D}}\right)=y_2^{2}。 \tag{9}$$

由(9)的第二式得出$\frac{\varepsilon^{h}+\bar{\varepsilon}^{h}}{2}=a^{2}$，代入(9)的第一式得

$$y_1^2=2\left(\frac{\varepsilon^h+\bar{\varepsilon}^h}{2}\right)^2-1=2a^4-1,$$

此给出（y_1，a）=（±1，±1），（±239，±13），前者给出 $h=0$，与$h>0$矛盾；后者给出$a^2=\frac{\varepsilon^h+\bar{\varepsilon}^h}{2}=169$，而

$$D\left(\frac{\varepsilon^h-\bar{\varepsilon}^h}{2\sqrt{D}}\right)^2=a^4-1=168\cdot170=2^4\cdot3\cdot5\cdot7\cdot17,$$

故$D=3\cdot5\cdot7\cdot17$，$\frac{\varepsilon^h-\bar{\varepsilon}^h}{2\sqrt{D}}=4$。但$D\equiv7,11\pmod{16}$，故这不可能。证毕。

在这个证明中，也可以不用Ljunggren关于方程$x^2+1=2y^4$的结果，而用上节的一些初等方法。

例如，由(9)第二式得出

$$\frac{\varepsilon^h+\bar{\varepsilon}^h}{2}=a^2,\quad \frac{\varepsilon^h-\bar{\varepsilon}^h}{2\sqrt{D}}=b^2,$$

故$a^4-Db^4=1$，此给出 $2\nmid a$，故由$2\mid u_0$ 及$\frac{\varepsilon^h+\bar{\varepsilon}^h}{2}=a^2$知 $2\mid h$，这由(9)的第一式知不可能（见[7]）。

然而，在使用Ljunggren 关于方程 $x^2+1=2y^4$ 的结果时，可以得出更为一般的定理。例如我们有：方程(1)的正整数解x,y 除$y=12428$（$D=3\cdot5\cdot7\cdot17$）外不满足$y^2=\frac{\varepsilon^{4m}-\bar{\varepsilon}^{4m}}{2\sqrt{D}}$，$m>0$。我们还有

定理10 设Pell方程$u^2-Dv^2=1$的基本解$u_0+v_0\sqrt{D}$满足$2\mid u_0$，则在方程$4X^4-DY^4=1$无整数解时，方程(1)没有满足$2\nmid x$的正整数解。

推论 1 设$D=pq$，p,q是素数，则在

1) $p\equiv 5 \pmod 8$，$q\equiv 7 \pmod 8$，$\left(\frac{q}{p}\right)=-1$且$qX^4-pY^4=2$无解时，或

2) $p\equiv 5 \pmod 8$，$q\equiv 3 \pmod 8$，$\left(\frac{q}{p}\right)=-1$ 且$pX^4-qY^4=2$无解时，方程(1)均无正整数解。

证 首先在1)、2)时容易验证$2|u_0$;其次从$4X^4-pqY^4=1$得$(2X^2-1)(2X^2+1)=pqY^4$，故 $p|2X^2\pm 1$，但$p\equiv 5 \pmod 8$，这不可能。于是由定理10 知方程(1)无$2\nmid x$ 的正整数解。

现设$2|x$，由(1)得出

$$x-1=pa^4,\ x+1=qb^4,\ 2\nmid ab,$$

或

$$x-1=qa^4,\ x+1=pb^4,\ 2\nmid ab,$$

或

$$x-1=a^4,\ x+1=pqb^4,\ 2\nmid ab,$$

或

$$x-1=pqa^4,\ x+1=b^4,\ 2\nmid ab,$$

消去x 依次有

$$qb^4-pa^4=2,\ 2\nmid ab,$$

或

$$pb^4-qa^4=2,\ 2\nmid ab,$$

或

$$pqb^4-a^4=2,\ 2\nmid ab,$$

或

$$b^4-pqa^4=2,\ 2\nmid ab。$$

后两式因为$p\equiv5\pmod8$知不可能。对前两式，在1）时，由于 $q\equiv7\pmod8$，故第二式给出$\left(\frac{p}{q}\right)=\left(\frac{2}{q}\right)=1$，与假设

$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=-1$矛盾，而第一式给出$qX^4-pY^4=2$有解，仍与假设矛盾。同理可证条件2）的情形。证毕。

由推论1可以有：丢番图方程 $x^2-5qy^4=1$（$q\equiv23,27\pmod{40}$是素数）无正整数解。

1982年，戴宗恕和曹珍富[32]进一步研究了$D=pq$的情形，证明了

定理11 设$D=pq$，p,q是不同的素数，则在

1） $p\equiv1\pmod8$，$q\equiv1\pmod4$，$\left(\frac{q}{p}\right)=-1$时，

或

2） $p\equiv37\pmod{40}$，$q\equiv13\pmod{40}$，$\left(\frac{q}{p}\right)=1$ 时，

方程(1)均无正整数解。

定理12 设$D=pq$，p，q是不同素数，则在

1） $p\equiv q\equiv5\pmod{12}$，$\left(\frac{q}{p}\right)=-1$时，

或

2） $p\equiv17\pmod{60}$，$q\equiv53\pmod{60}$时，

方程(1)除开在条件2）时$p=257$，$q=113$ 仅有解 $x=1658880001$，$y=3120$外，无其他的正整数解。

证明以上两个定理时，我们需要一个辅助的结果（见§3的定理7）：丢番图方程$4x^4-pqy^4=-1$（p,q是不同的素数）在$p\equiv1\pmod8$，$q\equiv1\pmod4$ 且$\left(\frac{q}{p}\right)=-1$ 时，或$p\equiv q\equiv$

$5(\bmod 8)$，且$\left(\frac{q}{p}\right)=1$时，均无正整数解。

定理13 设Pell方程$u^2-Dv^2=1$的基本解$u_0+v_0\sqrt{D}$满足$u_0\equiv1(\bmod 4)$，$\left(\frac{v_0}{u_0}\right)=-1$，则方程(1)无正整数解。

证 如果(1)有正整数解，则(1)给出

$$y^2=\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{D}},\quad n>0, \tag{10}$$

这里 $\varepsilon=u_0+v_0\sqrt{D}$，$\bar{\varepsilon}=u_0-v_0\sqrt{D}$，$\varepsilon\bar{\varepsilon}=1$。如果$2\nmid n$，则对(10)取模$u_0$得

$$y^2\equiv v_0(Dv_0^2)^{\frac{n-1}{2}}\equiv(-1)^{\frac{n-1}{2}}v_0(\bmod u_0),$$

由$u_0\equiv1(\bmod 4)$知上式给出$\left(\frac{v_0}{u_0}\right)=1$，与假设$\left(\frac{v_0}{u_0}\right)=-1$矛盾。于是$2|n$，设$n=2m$，则(10)给出

$$y^2=2\left(\frac{\varepsilon^m+\bar{\varepsilon}^m}{2}\right)\left(\frac{\varepsilon^m-\bar{\varepsilon}^m}{2\sqrt{D}}\right),$$

由此即得(7)或(8)式。对(7)，如果$2\nmid m$，则由(7)的第二式取模u_0知不可能。而$2|m$时，(7)的第一式左边是奇，与右边是偶矛盾。对(8)，如果$2\nmid m$，则在$u_0\equiv1(\bmod 8)$时，对(8)的第二式取模u_0可得矛盾结果，故$u_0\equiv5(\bmod 8)$。此时$u_0+1\equiv6(\bmod 8)$，所以存在素数$r\equiv3(\bmod 4)$，满足$r|u_0+1$，由$2\nmid m$，$r|u_0+1$，对(8)的第一式取模r得$y_1^2\equiv-1(\bmod r)$，此不可能。于是$2|m$，设$m=2h$，则(8)的第二式得出

$$\frac{\varepsilon^h+\bar{\varepsilon}^h}{2}=y_3^2,\quad \frac{\varepsilon^h-\bar{\varepsilon}^h}{2\sqrt{D}}=y_4^2,$$

此由后一式仍得出$2|h$。这个手续可以一直做下去，得出

$2^{\lambda}\mid n$，λ任意大，这就推出$n=0$，与$n>0$矛盾。证毕。

由定理13立即推出

推论 2 设 $D=s(st^2+2)$，s,t 均是正整数，且$s\equiv 1(\bmod 2)$，$t\equiv 2(\bmod 4)$，则方程(1)无正整数解。

证 由第五章§2定理4的推论知，Pell方程$u^2-s(st^2+2)v^2=1$的基本解为 $1+st^2+t\sqrt{D}$，即$u_0=1+st^2$，$v_0=t$。在$s\equiv 1(\bmod 2)$，$t\equiv 2(\bmod 4)$时，$u_0\equiv 1(\bmod 4)$，且

$$\left(\frac{v_0}{u_0}\right)=\left(\frac{t}{1+st^2}\right)=-1(\text{后一等号用到}1+st^2\equiv 5(\bmod 8)),$$

故由定理13知推论正确。证毕。

以上许多结果对方程(5)也成立。对定理 13 的证明方法还可以用来研究另外的一些二元四次丢番图方程。

最后，对于丢番图方程

$$x^4-Dy^4=1,\ D>0\text{且不是平方数}, \qquad (11)$$

可以证明

定理14 对每个D，方程(11)最多有一组正整数解。如果x_1,y_1是这样的解，且ε是 $Q(\sqrt{D})$ 中的基本单位数，$N(\varepsilon)=1$，则

$$x_1^2+y_1^2\sqrt{D}=\varepsilon\text{或}\varepsilon^2, \qquad (12)$$

且后一情形仅出现有限次。如果$N(\varepsilon)=-1$，则除$D=5$ 方程(11)没有正整数解。

Ljunggren已经证明，(12)中ε^2仅当$D=7140$时出现，这时有

$$239^2+26^2\sqrt{7140}=(169+2\sqrt{7140})^2=\varepsilon^2。$$

§3 丢番图方程$a^2x^4-Dy^2=-1$和$x^2-Dy^4=-1$

Cohn[3]在假设D使得方程 $X^2-DY^2=-4$ 有奇数解时，研究了丢番图方程

$$4x^4-Dy^2=-1 \tag{1}$$

的正整数解，这里$D>0$ 且不是平方数。证明了（参阅第二章§6）

定理 1 设D使得方程$X^2-DY^2=-4$有奇数解，则方程(1)除开$D=5$，$x=y=1$和$D=13$，$x=2$，$y=5$外，无其他的正整数解。

朱卫三[22]和曹珍富[23]证明了

定理 2 设 Pell 方程 $X^2-DY^2=-1$ 的基本解为$\delta=X_0+Y_0\sqrt{D}$，$X_0=df^2$，d无平方因子，则方程(1)有解的充要条件是$2|d$，且存在正整数x_1，y_1使得

$$2x_1^2+y_1\sqrt{D}=\delta^{\frac{d}{2}}。$$

当$D=p$是一个奇素数时，我们可以证明

定理 3 设$D=p\equiv1(\bmod 8)$是一个素数，则在$2^{\frac{p-1}{4}}\not\equiv(-1)^{\frac{p-1}{8}}(\bmod p)$或 $2p=a^2+b^2$，$a\equiv\pm3(\bmod 8)$，$b\equiv\pm3(\bmod 8)$时，方程(1)均无整数解。

证 在$D=p$是一个素数时，改写方程(1)为

$$(2x^2-2x+1)(2x^2+2x+1)=py^2,$$

故得出

$$2x^2\pm2x+1=pa^2,\quad 2x^2\mp2x+1=b^2。\tag{2}$$

先证 $2^{\frac{p-1}{4}}\not\equiv(-1)^{\frac{p-1}{8}}(\bmod\ p)$的情形。由(2)的两式相减得

$$\pm 4x = pa^2 - b^2,$$

这给出$\left(\frac{x}{p}\right)=1$。故存在整数$k$使得$k^2 \equiv x(\bmod p)$。现在对(1)取模$p$得

$$4k^2 \equiv -1(\bmod p),$$

两端乘$\frac{p-1}{8}$次方得到

$$2^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}}(\bmod p),$$

这与假设$2^{\frac{p-1}{4}} \not\equiv (-1)^{\frac{p-1}{8}}(\bmod p)$矛盾。再证$2p=a^2+b^2$，$a\equiv \pm 3(\bmod 8)$，$b\equiv \pm 3(\bmod 8)$的情形。此时由(2)的第一式得

$$(2x\pm 1)^2+1=2pa^2,$$

故由Lienen 定理（见第五章§3）知，上式不成立。证毕。

设$p=a^2+b^2\equiv 1(\bmod 8)$，$b\equiv 0(\bmod 4)$，则有

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{b}{4}}(\bmod p),$$

故对给定的素数$p\equiv 1(\bmod 8)$，条件$2^{\frac{p-1}{4}} \not\equiv (-1)^{\frac{p-1}{8}}(\bmod p)$容易判断。例如素数 $p=a^2+b^2$，$b\equiv 4(\bmod 8)$，$p\equiv 1(\bmod 16)$或$p=a^2+b^2$，$b\equiv 0(\bmod 8)$，$p\equiv 9(\bmod 16)$时均有$2^{\frac{p-1}{4}} \not\equiv (-1)^{\frac{p-1}{8}}(\bmod p)$。

Barrucand和Cohn[33]证明了：设素数$p\equiv 1(\bmod 8)$，则

$$\left(\frac{2}{p}\right)_4=1 \Longleftrightarrow \begin{cases} p=x^2+32y^2, & \text{当}p\equiv 1(\bmod 16); \\ p\ne x^2+32y^2, & \text{当}p\equiv 9(\bmod 16)。\end{cases}$$

$$\left(\frac{2}{p}\right)_4=-1 \Longleftrightarrow \begin{cases} p=x^2+32y^2, & \text{当}p\equiv 9(\bmod 16); \\ p\ne x^2+32y^2, & \text{当}p\equiv 1(\bmod 16)。\end{cases}$$

因此，他们证明了

定理 4 设$D=p\equiv 1 \pmod 8$是一个素数，则方程(1)仅当$p=U^2+32V^2$(U,V是整数）时有整数解。

例如$U^2=9$，$V^2=1$给出$p=41$，此时方程$4x^4-41y^2=-1$有整数解$x=4$，$y=5$。但$p=17$时不能表为U^2+32V^2的形式，故方程$4x^4-17y^2=-1$无整数解。

1985年，曹珍富和曹玉书[25]对D是两个素数乘积的情形证明了

定理 5 设$D=pq$，p,q是素数，则在$p=a^2+b^2\equiv 1 \pmod{16}$，$b\equiv 4 \pmod 8$或$p=a^2+b^2\equiv 9 \pmod{16}$，$b\equiv 0 \pmod 8$时，方程(1)无整数解。

例如，设$p=1^2+4^2=17\equiv 1 \pmod{16}$，故对任意素数$q$，方程$4x^4-17qy^2=-1$无整数解；设$p=3^2+8^2=73\equiv 9 \pmod{16}$，故对任意素数$q$，方程$4x^4-73qy^2=-1$没有整数解。

对于方程

$$4x^4-Dy^4=-1, \tag{3}$$

在$D=p$是一个素数时，(3)给出

$2x^2\pm 2x+1=py_1^4$，$2x^2\mp 2x+1=y_2^4$，$y=y_1y_2$，

此由第二式得出$(2x\mp 1)^2+1=2y_2^4$，因此有$2x\mp 1=\pm 1$，$y_2=\pm 1$和$2x\mp 1=\pm 239$，$y_2=\pm 13$。前者给出$x=-1,0,1$，故$p=5$，$y_1=\pm 1$，给出(3)有解$D=5$，$x=\pm 1$，$y=\pm 1$，后者给出$x=\pm 119$，± 120，故$py_1^4=113\cdot 257$，$541\cdot 137$，但由p是素数知，这不可能。这就有

定理 6 设$D=p$是一个奇素数，则方程(3)除开$D=5$，$x=\pm 1$，$y=\pm 1$外，无其他的整数解。

对D为两个素数乘积的情形，我们有

定理 7 设$D=pq$，p,q是素数，且$p\equiv 1 \pmod 8$，$q\equiv$

$1 \pmod 4$，$\left(\frac{q}{p}\right)=-1$或$p\equiv q\equiv 5 \pmod 8$，$\left(\frac{q}{p}\right)=1$，则方程(3)均没有整数解。

证 在$D=pq$时，(3)给出

$$2x^2\pm 2x+1=pqy_1^4，\ 2x^2\mp 2x+1=y_2^4, y=y_1y_2，\tag{4}$$

或

$$2x^2\pm 2x+1=py_1^4, 2x^2\mp 2x+1=qy_2^4，\ y=y_1y_2。\tag{5}$$

由$2x^2\mp 2x+1=y_2^4$易知(4)不可能。对(5)，由前两式得出

$$\pm 4x=py_1^4-qy_2^4,\tag{6}$$

这就给出$\left(\frac{x}{p}\right)=\left(\frac{q}{p}\right)$。在$p\equiv 1 \pmod 8$时，设$x=2^s x_1$，$s\geqslant 0$，$2\nmid x_1$，则由(5)的第一式取模$x_1$得

$$\left(\frac{x_1}{p}\right)=\left(\frac{p}{x_1}\right)=1,$$

故$\left(\frac{x}{p}\right)=\left(\frac{2^s x_1}{p}\right)=\left(\frac{2^s}{p}\right)\left(\frac{x_1}{p}\right)=1$。这就给出$\left(\frac{q}{p}\right)=1$，与假设$\left(\frac{q}{p}\right)=-1$矛盾。而在$p\equiv q\equiv 5 \pmod 8$时，此时$2\mid x$，由(5)知$x\equiv 2 \pmod 4$，设$x=4x_1+2$，对(5)的第一式取$2x_1+1$为模得出

$$\left(\frac{2x_1+1}{p}\right)=\left(\frac{p}{2x_1+1}\right)=1,$$

于是对(6)取模p得出

$$\left(\frac{x}{p}\right)=\left(\frac{q}{p}\right),$$

由$\left(\frac{q}{p}\right)=1$，$x=4x_1+2$，$\left(\frac{2x_1+1}{p}\right)=1$知，上式给出

$$1=\left(\frac{4x_1+2}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{2x_1+1}{p}\right)=\left(\frac{2}{p}\right),$$

但$p\equiv5(\bmod 8)$，故上式不成立。证毕。

对于丢番图方程

$$x^4-Dy^2=-1 \tag{7}$$

和

$$x^2-Dy^4=-1, \tag{8}$$

这里$D>0$且不是平方数。曹珍富[23]证明了

定理 8 设$\delta=X_0+Y_0\sqrt{D}$是Pell方程$X^2-DY^2=-1$的基本解，$X_0=dX_1^2$，d无平方因子。如果方程(7)有正整数解x,y，则必有$x^2+y\sqrt{D}=\delta^d$，$2\nmid d$。

由此可得

推论 方程(7)最多有一组正整数解。

Ljunggren[34]曾证明，在$2\nmid a$时，方程

$$a^2x^4-Dy^2=-1 \tag{9}$$

最多只有一组正整数解。由此可得出若干形为(9)的丢番图方程的全部正整数解，例如$9x^4-10y^2=-1$仅有$x=y=1$的正整数解。

对于方程(8)，利用二次剩余法，可以给出它有解的充要条件，即有

定理 9 设$\delta=X_0+Y_0\sqrt{D}$是Pell方程$X^2-DY^2=-1$的基本解，则(8)有正整数解的充要条件是Y_0为平方数，即存在正整数x_1，y_1使得$x_1+y_1^2\sqrt{D}=\delta$。

Ljunggren[35]证明了

定理10 设实二次域$Q(\sqrt{D})$上的整环为$Z[\sqrt{D}]$，如果$Q(\sqrt{D})$的基本单位数不是$Z[\sqrt{D}]$的基本单位数，则方程(8)最多有两组正整数解，并且这两组解可通过有限步计算得出。

这个定理的证明十分复杂，其证明思路如下：显然，如果Pell方程$X^2-DY^2=-1$无解，则方程(8)无解。故可设Pell方程$X^2-DY^2=-1$有解。于是整环$Z[\sqrt{D}]$的基本单位数为$\varepsilon=u+v\sqrt{D}$，令$\overline{\varepsilon}=u-v\sqrt{D}$，有$\varepsilon\overline{\varepsilon}=-1$，推出$2\nmid v$。现在由(8)式得出

$$x+y^2\sqrt{D}=\varepsilon^n,\quad x-y^2\sqrt{D}=\overline{\varepsilon}^n,\quad 2\nmid n>0,$$

故

$$y^2=\frac{\varepsilon^n-\overline{\varepsilon}^n}{2\sqrt{D}}=v\left(\frac{\varepsilon^n-\overline{\varepsilon}^n}{\varepsilon-\overline{\varepsilon}}\right)。\tag{10}$$

由定理9可设v是一个平方数，于是(10)给出

$$\frac{\varepsilon^n-\overline{\varepsilon}^n}{\varepsilon-\overline{\varepsilon}}=y_0^2,\tag{11}$$

我们在$Q(\sqrt{D})$的一个扩域上考虑(11)式，即有

$$\varepsilon^n-\overline{\varepsilon}^n=y_0^2(\varepsilon-\overline{\varepsilon}),$$

$$\varepsilon^{2n}+1=\varepsilon^{n-1}(\varepsilon^2+1)y_0^2,$$

$$(\varepsilon^n)^2-(\varepsilon^2+1)(y_0\varepsilon^{\frac{n-1}{2}})^2=-1。$$

故在环$Z[1,v\sqrt{D},\sqrt{\varepsilon^2+1},v\sqrt{D}\sqrt{\varepsilon^2+1}]$中，$\varepsilon^n+y_0\varepsilon^{\frac{n-1}{2}}\sqrt{\varepsilon^2+1}$是一个单位数，且$N(\varepsilon^n+y_0\varepsilon^{\frac{n-1}{2}}\sqrt{\varepsilon^2+1})=-1$。我们知道$Z[1,v\sqrt{D},\sqrt{\varepsilon^2+1},v\sqrt{D}\sqrt{\varepsilon^2+1}]$中有三个基本单位数，但Ljunggren证明仅使用它们中的二

个就足够了（他用[26]中的方法）。设η_1，η_2是这样的两个基本单位数，则有

$$\varepsilon^n + y_0\varepsilon^{\frac{n-1}{2}}\sqrt{\varepsilon^2+1} = \pm\eta_1^a\eta_2^b,\quad a,b\in Z。\qquad (12)$$

利用第三章的p-adic方法可以处理(12)式。

定理10最好的可能是给出了方程

$$x^2-2y^4=-1$$

仅有两组正整数解$(x,y)=(1,\ 1)$和$(239,\ 13)$。

此外，朱南等[21]也给出了方程(7)、(8)的一些结果，例如他们证明了在$D=25k^2\pm14k+2$，$k>0$，$k\equiv1$，2，5，6 (mod7)时，方程(7)无正整数解；在$D=25k^2\pm14k+2$，$k>0$，$2|k$，$k\equiv1,2,5,6$ (mod7) 时，方程(8)无正整数解。

Delone和Faddeev证明了

定理11 丢番图方程

$$x^4-Dy^4=\pm1 \qquad (13)$$

最多有一组正整数解，且如果整环$Z[\sqrt[4]{-4D}]$的基本单位数具有形式$\varepsilon=A^2+AB\sqrt[4]{-4D}+B^2\sqrt{-D}$，则(13)的正整数解由$x=A$，$y=B$给出。

Cohn[36]还用递推序列法较为系统地讨论了方程$x^2=Dy^4\pm1$，$x^2=Dy^4\pm4$的解（见§4）。

Ljunggren[67]证明了方程

$$x^2+4=Dy^4,\quad 2\nmid x,\quad D>0\text{不是平方数} \qquad (14)$$

最多有一组正整数解x，y。这个结果在求解方程$x^2+2^m=y^n$时将有应用（见第八章§2）。

§4 丢番图方程 $dy^2=ax^4+bx^2+c$

前几节讨论的二元四次丢番图方程都是

$$dy^2 = ax^4 + bx^2 + c \tag{1}$$

的特例，这里a，b，c，d是给定的整数。在前面章节提到的方程$x^4 - 3y^2 = -2$，$x^2 - 3y^4 = -2$，$x^2 - 27y^4 = -2$ 以及$3x^4 - 2y^2 = 1$都是(1)的具体例子。

1969年，Mordell[37] 讨论了方程

$$y^2 + k^2 = (lx^2 - h)(rx^2 - s) \tag{2}$$

的整数解，这里k不含 $4f+3$ 形的素因子。在 $lx^2 - h \equiv 3 \pmod 4$或$rx^2 - s \equiv 3 \pmod 4$时，(2)给出 $lx^2 - h < 0$或$rx^2 - s < 0$。再由l，h，r，s的关系，可找出方程(2)的全部解。例如对于方程

$$y^2 + 1 = (4x^2 - 17)(8x^2 - 10), \tag{3}$$

由于$4x^2 - 17 \equiv 3 \pmod 4$，故$4x^2 - 17 < 0$，这就给出$x = 0$，$\pm 1$，$\pm 2$，代入(3)检验知，(3)仅有解 $x = 0, \pm 1$。一般地，可以求出方程

$$y^2 + 1 = (4x^2 - 17)(rx^2 - s)$$

的全部整数解，这里r，s是任给的整数。

Ljunggren[38]曾用p—adic方法证明了

定理 1 丢番图方程

$$\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2} \tag{4}$$

仅有正整数解$(x, y) = (1,1)$，$(2,2)$和$(4,9)$。

Cassels[39]又给出定理1的一个用到四次域 $Q(\sqrt[4]{-2})$ 的性质的简单证明。由于令$2x-1 = X$，$2y-1 = Y$，则(4)化为$Y^2 = 2\left(\frac{X^2-1}{4}\right)^2 + 1$，故利用递推序列的方法有可能给出定理1的一个初等证明。

1971年，Cohn[40]用递推序列的方法证明了

定理 2 丢番图方程

$$y(y+1)(y+2)(y+3)=2x(x+1)(x+2)(x+3)$$

仅有正整数解$(x, y)=(4, 5)$。

以后，Ponnudurai[41]，宣体佐[42]和曹珍富[43]依次证明了

定理 3 丢番图方程

$$y(y+1)(y+2)(y+3)=3x(x+1)(x+2)(x+3)$$

仅有正整数解$(x,y)=(2,3)$和$(5,7)$。

定理 4 丢番图方程

$$y(y+1)(y+2)(y+3)=5x(x+1)(x+2)(x+3)$$

仅有正整数解$(x, y)=(1,2)$。

定理 5 丢番图方程

$$2y(y+1)(y+2)(y+3)=3x(x+1)(x+2)(x+3)$$

仅有正整数解$(x, y)=(8,9)$。

这些定理的证明虽然都是初等的，但远不是简单的。例如定理5中的方程可化为

$$\left(\frac{Y^2-5}{2}\right)^2-6\left(\frac{X^2-5}{4}\right)^2=-2, \tag{5}$$

这里$X=2x+3$，$Y=2y+3$。由(5)解出

$$\frac{Y^2-5}{2}+\frac{X^2-5}{4}\sqrt{6}=\frac{(2+\sqrt{6})^{2n+1}}{2^n}。 \tag{6}$$

记 $\alpha=2+\sqrt{6}$，$\beta=2-\sqrt{6}$，并令

$$V_n=\frac{\alpha^{2n+1}+\beta^{2n+1}}{2^{n+1}}, \quad U_n=\frac{\alpha^{2n+1}-\beta^{2n+1}}{2^{n+1}\sqrt{6}},$$

则(6)式给出

$$Y^2=2V_n+5, \quad X^2=4U_n+5。 \tag{7}$$

利用序列V_n，U_n的性质，就可求出(7)的全部解。但这决

不是件简单的事(解(7)的步骤完全类似于第二章§7的例1)。

Jeyaratnam[44]对每个$m\leqslant 30$，还找到了方程

$$y(y+m)(y+2m)(y+3m)=2x(x+m)(x+2m)(x+3m)$$

的全部正整数解。

Ljunggren[45]受Cohn方法（见[3]等）的启发，研究了丢番图方程

$$Ax^4-By^2=c \qquad (8)$$

的正整数解，这里A，B是正奇数，$c=1$或4。他证明了

定理 6 设$AX^2-BY^2=4$ 有奇数解，从而不妨设$X=a$，$Y=b$是它的一组正的奇数解。则丢番图方程

$$Ax^4-By^2=4 \qquad (9)$$

最多有两组正整数解。如果 $a=h^2$，$Aa^2-3=k^2$，则(9)有两组解$x=h$和$x=hk$。如果$a=h^2$，$Aa^2-3\neq k^2$，则$x=h$是(9)仅有的解。如果 $a=5h^2$，$A^2a^4-5Aa^2+5=5k^2$，则方程(9)仅有解$x=5hk$。其他情形没有解。

定理 7 设$AX^2-BY^2=4$ 有奇数解，则丢番图方程

$$Ax^4-By^2=1 \qquad (9')$$

最多有一组正整数解x,y。如果$x=x_1$，$y=y_1$是（9′)的一个解，则

$$x_1^2\sqrt{A}+y_1\sqrt{B}=\left(\frac{a\sqrt{A}+b\sqrt{B}}{2}\right)^3,$$

这里a,b是$AX^2-BY^2=4$ 的正奇数解。

Cohn[3]在方程$X^2-DY^2=-4$有奇数解时，研究了方程 $y^2=Dx^4\pm 4$ 和$Dy^2=x^4+4$ 的解，例如他证明了方程$Dy^2=x^4+4$在$D=5$时仅有正整数解$x=y=1$，$x=y=2$，而在$D\neq 5$时最多只有一组正整数解x，y。

在方程$X^2-DY^2=-4$没有奇数解，而方程$X^2-DY^2=$

4 有奇数解时，Cohn[6] 证明了方程$Dy^2=x^4-4$最多有一组正整数解，而方程$y^2=Dx^4+4$最多有两组正整数解。

1972年，Cohn[36]利用递推序列法给出了几个丢番图方程的一个较为详细地讨论，他证明了如下的几个定理。

定理 8 设$D=dN^2$，d使得方程$X^2-dY^2=-4$有奇数解，则四个丢番图方程$x^2=Dy^4\pm1$，$x^2=Dy^4\pm4$都最多只有一个正整数解，并且它们中间除开下面的情形外，最多有两个方程对同一D有解：

1） 当$D=5$时，四个方程总共有五个解：$y=1$是方程$x^2=5y^4-1$，$x^2=5y^4\pm4$的解；$y=2$是方程$x^2=5y^4+1$的解；$y=12$是方程$x^2=5y^4+4$的解。

2） 当$D=20$时，四个方程共有三个解：$y=1$是$x^2=20y^4-4$的解；$y=2$是$x^2=20y^4+4$的解；$y=6$是$x^2=20y^4+1$的解。

定理 9 设$D=dN^2$，d使得$X^2-dY^2=4$有奇数解，但使得$X^2-dY^2=-4$没有奇数解，则方程$x^2=Dy^4+1$和$x^2=Dy^4+4$中最多有两个正整数解，且它们最多有一个是共同的解。

定理10 设d使得$X^2-dY^2=-4$有奇数解，则对任意正整数N，四个方程$N^2x^4-dy^2=\pm1$，±4中间除开两个例外情形，最多有一个正整数解：

1） 当$d=5$，$N=1$时，我们得到仅有的三个解：$x=1$或2是$x^4-5y^2=-4$的解；$x=3$是$x^4-5y^2=1$的解。

2） 当$d=5$，$N=2$时，仅有两个解：$x=1$是$4x^4-5y^2=-1$的解；$x=3$是$4x^4-5y^2=4$的解。

定理11 设d使得$X^2-dY^2=4$有奇数解，而使得$X^2-dY^2=-4$没有奇数解，则对任意正整数N，方程

$N^2x^4-dy^2=1$ 和 $N^2x^4-dy^2=4$ 中间最多有一个正整数解。

这些结果也可以用Pell方程法来证明(参阅第二章§6)[46]。

1979年，柯召和孙琦[46]证明了

定理12 设 D 使得方程 $X^2-DY^2=-4$ 有奇数解，D 是一个奇素数，则方程 $Dy^2=x^4+4$ 除开 $D=5$ 时仅有解 $x=y=1$，$x=y=2$ 和 $D=13$ 时仅有解 $x=6$，$y=10$ 外，无其他的正整数解。

1983年，姚琦[47]给出 D 使得方程 $X^2-DY^2=-4$ 有奇数解且 $D\leqslant 200$ 时方程 $Dy^2=x^4+4$ 的全部解，她证明了此时除 $D=5$，13，85外，无正整数解。

Velupillai[48]研究了方程 $y^2=Dx^4+4$ 的一些奇数解，例如他证明了在 $D\leqslant 181$ 时，仅当 $D=5$，21，45，77，85，117或165时，方程 $y^2=Dx^4+4$ 有奇数解。

Cohn[49]在方程 $X^2-DY^2=-4$ 有奇数解时，利用递推序列法研究了丢番图方程

$$x^4-Dy^2=k,$$
$$x^2-Dy^4=k, \tag{10}$$

的正整数解，例如他证明了

1) 方程 $x^4-5y^2=-44$ 仅有正整数解 $(x,y)=(1,3)$，(3，5)和(47，1453)；

2) 方程 $x^4-5y^2=11$ 仅有正整数解 $(x,y)=(2,1)$ 和(4，7)；

3) 方程 $x^2-5y^4=44$ 仅有正整数解 $(x,y)=(7,1)$；

4) 方程 $x^2-5y^4=11$ 仅有正整数解 $(x,y)=(4,1)$ 和(56，5)；

5) 方程 $x^2-5y^4=-44$ 仅有正整数解 $(x,y)=(6,2)$，

(19, 3)和(181, 9)。

1983年，Tzanakis[50]利用递推序列法证明了

定理13 两个丢番图方程

$$y^2-2x^4=17,\quad y^2-8x^4=17$$

在$x\equiv 0(\bmod 8)$时均无正整数解。

定理14 丢番图方程$y^2-2x^4=41$无$x\equiv 0(\bmod 8)$的整数解，而丢番图方程$y^2-8x^4=41$无$x\equiv 0(\bmod 4)$的整数解。

定理15 两个丢番图方程

$$y^2-2x^4=73,\quad y^2-8x^4=73$$

在$2|x$且$x\not\equiv 0(\bmod 3)$时均无整数解。

定理16 丢番图方程$y^2-2x^4=89$在$x\equiv 0(\bmod 16)$时无整数解，而丢番图方程$y^2-8x^4=89$在$2|x$且$x\not\equiv 0(\bmod 5)$时无整数解。

定理17 丢番图方程 $y^2-2x^4=97$在$x\equiv 0(\bmod 8)$时无整数解，而丢番图方程$y^2-8x^4=97$在$x\equiv 0(\bmod 4)$时无整数解。

这些定理的一般证明思路为：设$c=1$或2，$p=17,41,73$，89或97，则定理13—17中的几个方程均可化为

$$y^2-2c^2x^4=p。\tag{11}$$

由于方程$y^2-Dx^2=\pm p$在$p\nmid 2D$时有两个结合类（见第五章§3），故(11)给出

$$y+cx^2\sqrt{2}=\pm\varepsilon^r(a+b\sqrt{2})\text{或}\pm\varepsilon^r(a-b\sqrt{2}),\quad r\in Z,\tag{12}$$

这里$a^2-2b^2=p\equiv 1(\bmod 8)$，从而$2\nmid a$，$2|b$，并且$\varepsilon=1+\sqrt{2}$。令

$$u_n=\frac{\varepsilon^n-\bar{\varepsilon}^n}{\varepsilon-\bar{\varepsilon}},$$

这里$\bar{\varepsilon} = 1-\sqrt{2}$，则有递推序列

$$u_0=0,\ u_1=1,\ u_{n+2}=2u_{n+1}+u_n \text{且} u_{-n}=(-1)^{n+1}u_n。\tag{13}$$

现在，(12)的第一情形给出$\eta(y+cx^2\sqrt{2})=\varepsilon^r(a+b\sqrt{2})$和$\eta(y-cx^2\sqrt{2})=\bar{\varepsilon}^r(a-b\sqrt{2})$，$\eta=\pm1$，于是

$$\begin{aligned}\pm cx^2(\varepsilon-\bar{\varepsilon}) &= a(\varepsilon^r+\bar{\varepsilon}^r)+\frac{b}{2}(\varepsilon-\bar{\varepsilon})(\varepsilon^r+\bar{\varepsilon}^r)\\ &= \frac{a}{2}(\varepsilon+\bar{\varepsilon})(\varepsilon^r-\bar{\varepsilon}^r)\\ &\quad+\frac{b}{2}(\varepsilon-\bar{\varepsilon})(\varepsilon^r+\bar{\varepsilon}^r),\end{aligned}$$

由此即得

$$\begin{aligned}\pm 2cx^2(\varepsilon-\bar{\varepsilon}) &= (a+b)(\varepsilon^{r+1}-\bar{\varepsilon}^{r+1})\\ &\quad+(a-b)\varepsilon\bar{\varepsilon}\ (\varepsilon^{r-1}-\bar{\varepsilon}^{r-1})\\ &= (a+b)(\varepsilon^{r+1}-\bar{\varepsilon}^{r+1})\\ &\quad-(a-b)(\varepsilon^{r-1}-\bar{\varepsilon}^{r-1}),\end{aligned}$$

两端除以 $\varepsilon-\bar{\varepsilon}$ 得出

$$\pm 2cx^2=(a+b)u_{r+1}-(a-b)u_{r-1}。$$

同理，由(12)的后一情形得出

$$\pm 2cx^2=(a-b)u_{r+1}-(a+b)u_{r-1}。$$

令

$$w_n=(a+b)u_{n+1}-(a-b)u_{n-1},$$
$$z_n=(a-b)u_{n+1}-(a+b)u_{n-1},$$

则由(13)式知

$$w_0=2b,\ w_1=2(a+b),\ w_{n+2}=2w_{n+1}+w_n,$$
$$w_{-n}=(-1)^{n+1}z_n,$$

$$z_0=-2b,\ z_1=2(a-b),\ z_{n+2}=2z_{n+1}+z_n,$$

$$z_{-n}=(-1)^{n+1}w_n。$$

然后利用递推序列的性质来解方程 $2cx^2=\pm w_r$ 或 $2cx^2=\pm z_r$。由 $2cx^2=-w_r$ 推出 $r<0$，令 $r=-s$，$s>0$，则 $2cx^2=-w_r=-w_{-s}=-(-1)^{s-1}z_s=(-1)^s z_s$，因为 $z_s>0$，所以 $2|s$ 且 $2cx^2=z_s$。同理由 $2cx^2=-z_r$ 可推出 $2cx^2=w_s$，$2|s>0$。于是只需解方程 $2cx^2=w_r$，$2cx^2=z_r$，关于 w_r，z_r 的一个很有用的一般性质是

$$w_{n+2mt}\equiv(-1)^{mt}w_n(\bmod u_m),$$

$$z_{n+2mt}\equiv(-1)^{mt}z_n(\bmod u_m)。$$

这样便可仿第二章§7的方法来证明上述的定理13—17。

1986年，Tzanakis[51]对丢番图方程(10)证明了，设 $k>0$，$D>0$ 都不是平方数，则可找到有限个形为 $g(u,v)=A^2$，u，$v\in Z$ 的方程，这里 A 是一个已知整数，g 是整数二元四次型且 $g(\theta,1)=0$ 恰有两个实根。如果我们找到这些方程的全部解，则方程(10)的全部解便可找到。从(10)找有限个方程 $g(u,v)=A^2$，我们在第三章§1的末尾已经给出寻找方法。对于特殊的例子，可以用这种方法给出形为(10)的全部整数解。例如，Tzanakis证明了

定理18 丢番图方程 $x^2-3y^4=46$ 仅有的整数解由 $(|x|,|y|)=(7,1),(17,3)$ 给出。

在证明定理18时，需要解决方程

$$x^4-4x^2y^2+y^4=46, \tag{14}$$

可证明(14)仅有整数解 $(|x|,|y|)=(1,3),(3,1)$。对于丢番图方程

$$x^4-4x^2y^2+y^4=n, \tag{15}$$

曾引起过许多人的兴趣，例如Erdös，Graham和Selfridge

等[52]均有工作。目前，人们已经证明：在$|n|\leqslant 100$时，仅当$n\in\{-47,\ -32,\ -2,\ 1,16,\ 46,\ 81\}$时，方程(15)有解。

最后，由于Tzanakis 关于定理18的证明远不是初等的（尽管不十分复杂），因此我们希望给出一个初等证明，并且我们相信用递推序列的方法能够做到这一点。

§5 丢番图方程$x^4+kx^2y^2+y^4=z^2$

对丢番图方程

$$x^4+kx^2y^2+y^4=z^2,\quad xy\neq 0 \tag{1}$$

的研究已有很长的历史。例如Fermat 就已经用无穷递降法（见第二章§3）证明了$k=0$时方程（1）无整数解。从Dickson[53]著《数论史》第Ⅱ卷可知，Euler，Legendre，Lucas等对方程(1)均有过工作。我们在第二章的§3 用无穷递降法证明了$k=-1$时方程(1)仅有解$x=\pm 1$，$y=\pm 1$；$k\in\{1,\pm 6\}$时方程(1)无解；$k=14$时方程(1)仅有解$x=\pm 1, y=\pm 1$。1914年，Pocklington[54]给出方程(1) 无解的6个判定定理，并在总结前人结果的基础上，列出了-100到100间的56个k值使方程(1)无解(为方便计，以下简称使方程(1)无解的$k\in$P表）。1978年，Sinha[55]利用Mersenne 素数的性质给出了一个新$k=30\in P$表。

1983年，张明志[56]利用分解因子法给出判定方程(1)无解的一系列命题。从(1) 可不失一般设$(x,y)=1$，$x>0$，$y>0$，将(1)变形为

$$y^2(kx^2+y^2)=(z+x^2)(z-x^2), \tag{2}$$

先看$k>2$的情形。令$\dfrac{\lambda}{\mu}=\dfrac{y^2}{z+x^2}=\dfrac{z-x^2}{kx^2+y^2}$，其中$\lambda$，$\mu>0$，

$(\lambda,\mu)=1$。于是(2)式给出

$$\begin{cases}\lambda x^2-\mu y^2+\lambda z=0,\\(\lambda k+\mu)x^2+\lambda y^2-\mu z=0,\end{cases}$$

由此知 $\dfrac{x^2}{\Delta_1}=\dfrac{y^2}{\Delta_2}=\dfrac{z}{\Delta_3}$，这里

$$\Delta_1=\begin{vmatrix}-\mu & \lambda\\ \lambda & -\mu\end{vmatrix}=\mu^2-\lambda^2,$$

$$\Delta_2=\begin{vmatrix}\lambda & \lambda\\ -\mu & \lambda k+\mu\end{vmatrix}=2\lambda\mu+k\lambda^2,$$

$$\Delta_3=\begin{vmatrix}\lambda & -\mu\\ \lambda k+\mu & \lambda\end{vmatrix}=\lambda^2+k\lambda\mu+\mu^2。$$

因x^2，y^2，z两两互素，故得出

$$\begin{cases}\xi x^2=\mu^2-\lambda^2 & (3)\\ \xi y^2=2\lambda\mu+k\lambda^2 & (4)\\ \xi\ z=\lambda^2+k\lambda\mu+\mu^2 & (5)\end{cases}$$

这里 $\xi=(\mu^2-\lambda^2,\ 2\lambda\mu+k\lambda^2)$。因 $(\lambda,\mu)=1$，由(3)得 $(\xi,\ \lambda)=(\xi,\ \mu)=1$，于是$\xi=(\mu^2-\lambda^2,\ 2\mu+k\lambda)$。令 $\xi_1=(\xi,\ \mu+\lambda)$，$\xi=\xi_1\xi_2$，因$\xi_1\xi_2|(\mu+\lambda)(\mu-\lambda)$，故 $\xi_2|\dfrac{\mu+\lambda}{\xi_1}(\mu-\lambda)$，而$(\xi_1,\ \dfrac{\mu+\lambda}{\xi_1})=1$，故$\xi_2|\mu-\lambda$。由此即知$\xi_1|k-2$，$\xi_2|k+2$。令$k-2=\xi_1\eta_1$，$k+2=\xi_2\eta_2$。这样可使(3)—(5)联列的方程组进一步得到展开。

同理，在$k<-2$时也可以类似讨论。通过这些讨论，张明志给出了

定理 1 设 $k\equiv3(\text{mod}8)$，且$k-2$为素数，$k+2=pq$，这里 $p\equiv3(\text{mod}8)$，$q\equiv7(\text{mod}8)$均为素数，则方程(1)无整数解。

定理 2 设$k\equiv7(\text{mod}8)$，若$k-2$与$k+2$ 均为素数，则

方程(1)无整数解。

还有几个结果，可以给出一些k值使得方程(1)无整数解。利用这些结果，可以给出18个新的k值$\in P$表。

关于方程(1)，Aubry[53]在1911年曾猜想：当$|k|=\sqrt{pq+4}$，p,q均为素数(即$|k+2|$和$|k-2|$均为素数)时，若$0<k\not\equiv 3(\bmod 8)$或$0>k\equiv 3(\bmod 8)$，则方程(1)无整数解。

由Pocklington[54]和张明志[56]的结果可推出Aubry猜想是正确的。但是他们的方法都未能导出Aubry的全部断言。

1986年，郑德勋[57]给出猜想的一个完整的自给的证明。他证明了

定理 3 当$|k+2|$和$|k-2|$均为素数时，若$0>k\equiv 3$(mod8)或$0<k\equiv 1,5,7$(mok8)，则(1)无整数解。

同时，郑德勋还证明了Aubry断言对k值模8分类而言是不可改进的。

目前，对于$|k|\leqslant 100$时方程(1)是否可解已全部得到解决，例如在$0\leqslant k\leqslant 100$时，$P$表的$k$值仅有：0,1,3,4,5,6,9,10,11,15,18,19,20,21,22,25,28,29,30,32,35,37,39,40,43,45,46,50,51,53,54,58,59,65,69,70,72,74,75,76,80,81,82,88,91,93,97。

1987年，郑德勋[58]对方程(1)的可解性提供了一个新的判别法，且在有解时可具体地给出一个或多个互素的解来。

定理 4 设$k>2$，且

$$k-2=a^2+b^2,\quad k+2=a_1^2+b_1^2, \tag{6}$$

则当存在$|\lambda_1|=|\lambda_2|=1$使

$$d_1=a+\lambda_1 a_1,\quad d_2=b+\lambda_2 b_1 \tag{7}$$

$$d_1^2+d_2^2=d^2,\quad d_1d_2\neq 0 \tag{8}$$

时，方程(1)有解

$$x=2d'|ad_2'-bd_1'|,$$

$$y=|(ad_1'+bd_2')(\lambda_1\lambda_2a_1d_1'+b_1d_2')|,$$

$$z=\frac{1}{4}|(k-2)(b_1d_2'+\lambda_1\lambda_2a_1d_1')^4$$

$$-(k+2)bd_2'+ad_1')^4|,$$

这里的 $d_1'=\dfrac{d_1}{(d_1,d_2)}$，$d_2'=\dfrac{d_2}{(d_1,d_2)}$，$d'=\dfrac{d}{(d_1,d_2)}$。

证 由于容易验证

$$[k(u^2-v^2)^2-2(u^4-v^4)]^2+k[k(u^2-v^2)^2-2(u^4-v^4)](2uv)^2+(2uv)^4=[(k-2)u^4-(k+2)v^4]^2,$$

故只要证明，在定理4的条件下可取 $uv\neq 0$ 使得

$$|k(u^2-v^2)^2-2(u^4-v^4)|=|u^2-v^2||(k-2)u^2-(k+2)v^2|$$

为一非零平方数即可。为此，令 $st\neq 0$ 使

$$\begin{cases}u^2-v^2=s^2,\\(k-2)u^2-(k+2)v^2=t^2,\end{cases}$$

由此得出

$$\begin{cases}(k-2)s^2=t^2+4v^2,\\(k+2)s^2=t^2+4u^2。\end{cases}$$

由假设条件(6)式知，对任意整数 ξ，η，ξ_1，η_1 和 $\varepsilon_i=\pm 1$ $(i=1,2)$，上式可有解

$$s=\xi^2+\eta^2,\ t=a(\xi^2-\eta^2)-2\varepsilon_1b\xi\eta,\ 2v=b(\xi^2-\eta^2)+2\varepsilon_1a\xi\eta;$$

$$s=\xi_1^2+\eta_1^2,\ t=a_1(\xi_1^2-\eta_1^2)-2\varepsilon_2b_1\xi_1\eta_1,$$

$$2u=b_1(\xi_1^2-\eta_1^2)+2\varepsilon_2a_1\xi_1\eta_1,$$

故以下只要证在定理条件下必可选得ξ,η，ξ_1，η_1和$\varepsilon_i=\pm1$ $(i=1,2,3)$使得$stuv\neq0$，且

$$\xi^2+\eta^2=\xi_1^2+\eta_1^2,$$

$$a(\xi^2-\eta^2)-2\varepsilon_1 b\xi\eta=\varepsilon_3[a_1(\xi_1^2-\eta_1^2)-2\varepsilon_2 b_1\xi_1\eta_1]。$$

为此令$\xi=\xi_1$，$\eta=\eta_1$，则后一式给出

$$f(\xi,\eta)=(a-\varepsilon_3 a_1)\xi^2-(a-\varepsilon_3 a_1)\eta^2$$
$$-2\varepsilon_1(b-\varepsilon_1\varepsilon_2\varepsilon_3 b_1)\xi\eta=0$$

再取$\varepsilon_3=-\lambda_1$，$\varepsilon_1=1$，$\varepsilon_2=\lambda_1\lambda_2$，则由假设条件(7)有

$$f(\xi,\eta)=d_1\xi^2-2d_2\xi\eta-d_1\eta^2=0。$$

再由假设条件(8)知，上式可写为

$$d_1 f(\xi,\eta)=(d_1\xi-d_2\eta)^2-d^2\eta^2=0,$$

由此可知$\xi=d_2-d_1$，$\eta=d_1$满足$f(\xi,\eta)=0$。下面只要验证按这种方法选取的$stuv\neq0$即可。这一步我们留给读者去完成。证毕。

由定理4可推出

推论 设$t_0=1$，$t_1=7$，$t_{n+2}=6t_{n+1}-t_n$。则当$n>0$，$k=(t_n\pm1)^2+2$时，方程(1)有解。

证 因为此时有$k-2=(t_n\pm1)^2+0^2$，$k+2=(t_n\pm1)^2+2^2$，故取$a=t_n\pm1$，$b=0$，$a_1=2$，$b_1=t_n\pm1$，$\lambda_1=\mp1$，$\lambda_2=1$，则有$d_1=t_n\pm1\mp2=t_n\mp1$，$d_2=t_n\pm1$。因为$n>0$时有$t_n\geqslant7$，故$d_1d_2\neq0$，且$d_1^2+d_2^2=(t_n\mp1)^2+(t_n\pm1)^2=2(t_n^2+1)$。又因

$$t_n=\frac{\varepsilon^{2n+1}+\bar{\varepsilon}^{2n+1}}{2},\quad \varepsilon=1+\sqrt{2},\quad \bar{\varepsilon}=1-\sqrt{2},$$

故有$u_n=\dfrac{\varepsilon^{2n+1}-\bar{\varepsilon}^{2n+1}}{2\sqrt{2}}$使得$t_n^2-2u_n^2=-1$，于是知

$$d_1^2+d_2^2=2(t_n^2+1)=(2u_n)^2。$$

这就验证定理4的条件全部得到满足，证毕。

对于一般的丢番图方程

$$ax^4+bx^2y^2+cy^4=dz^2,\ (x,y)=1,\ xy\neq 0,\quad (9)$$

利用初等方法还可以得出一些结果。例如 $d=a$时，(9)化为

$$y^2(bx^2+cy^2)=a(z-x^2)(z+x^2),$$

可利用分解因子法（见第二章§2）加以研究；或者，(9)的左端可分解，化为

$$(a_1x^2+b_1xy+c_1y^2)(a_2x^2+b_2xy+c_2y^2)=dz^2,$$

根据唯一分解定理使问题得到展开。在这方面，Sinha[59]证明了当$(a,b,c,d)=(3,10,3,3)$或$(1,3,9,1)$时，方程(9)无解；当$(a,b,c,d)=(3,-2,-1,3)$或$(1,1,1,3)$时，方程(9)仅有解$x^2=y^2=1$；当$(a,b,c,d)=(-1,10,-9,3)$时，方程(9)仅有解$y^2=1$，$x^2=1$或9。

此外，对丢番图方程

$$ax^4+by^4=cz^2,\ (x,y)=1,$$

也有过一些工作[54]，例如Mordell[60]利用分解因子法和无穷递降法证明了：设

1） $d=p$，$p\equiv 7$，$11 \pmod{16}$；或

2） $d=2p$，$p\equiv\pm 3 \pmod 8$；或

3） $d=4p$，$p\equiv\pm 3$，$-5 \pmod{16}$；或

4） $d=-p$，$p\equiv\pm 3$，$-5 \pmod{16}$；

则丢番图方程

$$x^4+dy^4=z^2,\ (x,y)=1\quad (10)$$

无正整数解。

同样方法可研究方程(10)当 $d=pq$，$2pq$或$4pq$，p，q是不同的奇素数时的解。

§6 一些四元四次丢番图方程

四元四次丢番图方程

$$ax^4+by^4+cz^4=dw^4,\quad abcd\neq 0 \tag{1}$$

的研究是很困难的。Euler有一个著名的猜想是:丢番图方程

$$x^4+y^4+z^4=w^4,\quad xyz\neq 0 \tag{2}$$

没有整数解。Ward[6 1],[6 2] 证明了当$w<10000$时 Euler猜想是正确的。Lander, Parkin 和 Selfridge[6 3]把w 的上界推到220000。

1981年，Guy[6 4]指出，不仅对方程(2)，甚至连丢番图方程

$$x^4+y^4+z^4=w^2 \tag{3}$$

是否有解也未解决。1983年，郑格于[6 5]找到了方程(3)的无穷多组解：

$$\begin{cases} x=a^4-b^4\\ y=2a^3b-2ab^3\\ z=2a^3b+2ab^3\\ w=(a^2+b^2)^4-4a^2b^2(a^2-b^2)^2 \end{cases}$$

(参阅第二章§2)。但方程(3)的全部整数解的表达式仍没有找到。最近，在日本京都大学主办的“丢番图问题”(1988年2月)会议上*，Noam D. Elkies利用椭圆曲线证明了方程(2)有无穷多组解，并且用计算机找到了一组解：$x=2682440$，$y=15365639$，$z=18796760$，$w=20615673$。这就否定了Euler猜想。

现在我们给出方程(1) 在两个特殊情况下构造部分解的

---

* 见《中国数学会通讯》1988年6月（第2期），第11页。

方法。

Ⅰ．对于丢番图方程

$$x^4+y^4=z^4+w^4, \quad (4)$$

令 $x=at+c$，$y=bt-d$，$z=at+d$，$w=bt+c$，这里a,b,c,d是参数，代入(4)得

$$(at+c)^4+(bt-d)^4=(at+d)^4+(bt+c)^4。\quad (5)$$

由(5)展开知，含 t^4项与常数项两端分别相等。现令含 t^3的两端系数相等，得出

$$c(a^3-b^3)=d(a^3+b^3),$$

显然此在$c=a^3+b^3$，$d=a^3-b^3$时成立，于是在$c=a^3+b^3$，$d=a^3-b^3$时(5)化为

$$6(a^2c^2+b^2d^2)t^2+4(ac^3-bd^3)t$$
$$=6(a^2d^2+b^2c^2)t^2+4(ad^3+bc^3)t,$$

两端除以$2t$得出

$$3t(a^2-b^2)(c^2-d^2)=2(ad^3-ac^3+bc^3+bd^3)。$$

把$c=a^3+b^3$，$d=a^3-b^3$代入上式并解出 t，于是得到方程(4)的无穷多组解

$$x=a^7+a^5b^2-2a^3b^4+3a^2b^5+ab^6,$$
$$y=a^6b-3a^5b^2-2a^4b^3+a^2b^5+b^7,$$
$$z=a^7+a^5b^2-2a^3b^4-3a^2b^5+ab^6,$$
$$w=a^6b+3a^5b^2-2a^4b^3+a^2b^5+b^7。$$

Ⅱ．可以证明丢番图方程

$$x^4+y^4+4z^4=w^4 \quad (6)$$

有无穷多组整数解，例如，

$$x=a^4-2b^4,\ y=2a^3b,\ z=2ab^3,\ w=a^4+2b^4。\quad (7)$$

构造这组解的方法是，把求(6)的整数解化为求方程

$$X^4+Y^4+4Z^4=1 \quad (8)$$

的有理解。令

$$X^2+2YZ=1,$$

则

$$Y^4+4Z^4=1-X^4=1-(1-2YZ)^2,$$

$$(Y^2+2Z^2)^2=4YZ,$$

$$Y^2+2Z^2=2\sqrt{YZ}。$$

令$Y=t^2Z$，t为有理数，则有

$$(t^4+2)Z=2t,\quad Z=\frac{2t}{t^4+2},\quad Y=\frac{2t^3}{t^4+2}。$$

因为

$$(Y^2-2Z^2)^2=4YZ(1-2YZ)=4YZX^2,$$

故

$$X=\frac{Y^2-2Z^2}{2\sqrt{YZ}}=\frac{t^4-2}{2t}Z=\frac{t^4-2}{t^4+2}。$$

这就得出(8)有有理解

$$X=\frac{t^4-2}{t^4+2},\quad Y=\frac{2t^3}{t^4+2},\quad Z=\frac{2t}{t^4+2}。$$

令$t=\frac{a}{b}$，$a,b\in Z$，$b\neq 0$，则(8)的有理解为

$$X=\frac{a^4-2b^4}{a^4+2b^4},\quad Y=\frac{2a^3b}{a^4+2b^4},\quad Z=\frac{2ab^3}{a^4+2b^4}。$$

于是给出(6)有解(7)。

由于(6)可化为

$$(y^2+2yz+2z^2)(y^2-2yz+2z^2)=(w^2-x^2)(w^2+x^2),$$

故用分解因子法，可给出方程(6)的一些新解。

最后，对五元四次丢番图方程

$$x_1^4+x_2^4+x_3^4+x_4^4=x_5^4,\quad (x_1,\cdots,x_5)=1, \tag{9}$$

1911年，Norrie[66]找到了一组解

$$30^4+120^4+272^4+315^4=353^4。$$

现在的问题是，方程（9）有参数解吗？能给出（9）的全部解吗？这是一个不易回答的问题。

参 考 文 献

[1] Ljunggren, W.,Arch.Math. Naturvid.45, No. 5 (1942), 61—70。

[2] Ljunggren, W., J. London Math. Soc., 41(1966), 542—544.

[3] Cohn, J.H.E., Proc. London Math.Soc., 16 (1966), 153—166.

[4] Cohn, J. H.E., Addendum, Proc.London Math. Soc., 17 (1967), 381.

[5] Bumby, R. T., Math. Scand.,21 (1967), 144—148.

[6] Cohn, J. H. E.,Math.Scand.,21 (1967), 61—70.

[7] 柯召，孙琦，四川大学学报（自然科学版），1 (1975), 57—61。

[8] Cohn, J. H. E., Quart. J. Math. Oxford (3), 26 (1975), 279—281.

[9] 柯召，孙琦，四川大学学报（自然科学版），4 (1979), 5--9。

[10] 柯召，孙琦，四川大学学报（自然科学版），2 (1983), 1—3。

[11] 柯召，孙琦，科学通报，16 (1979), 721—723。

［12］ 柯召，孙琦，数学学报，6（1980），922—926。
［13］ 柯召，孙琦，四川大学学报（自然科学版），3（1980），37—43。
［14］ 柯召，孙琦，数学年刊，1（1980），83—88。
［15］ 曹珍富，哈尔滨工业大学学报，4（1981），53—58。
［16］ 曹珍富，哈尔滨工业大学学报，2（1983），133—138。
［17］ 曹珍富，数学杂志，3（1983），227—235。
［18］ 康继鼎，万大庆，周国富，数学研究与评论，1（1983），83—84。
［19］ 贾广聚，曹珍富，哈尔滨师范大学学报（自然科学版），1（1985），78—82。
［20］ 康继鼎，周国富，万大庆，赵立人，中国科学技术大学学报，2（1982），119—121。
［21］ 朱南，罗明，胡世明，四川大学学报（自然科学版），4（1984），105—106。
［22］ 朱卫三，数学学报，5（1985），681—683。
［23］ 曹珍富，自然杂志，2（1987），151。
［24］ 曹珍富，哈尔滨工业大学科研报告，253（1982），8—9。
［25］ 曹珍富，曹玉书，黑龙江大学自然科学学报，1（1985），22—27，MR 87b：11021。
［26］ Ljunggren, W., Skr. Norske Vid—Akad. Oslo I Mat.—Naturv. KI. 1936, No. 12.
［27］ Mordell, L.J., J. London Math. Soc., 39 (1964), 161—164.
［28］ Cohn, J.H.E., J. London Math. Soc., 42

(1967), 475—476.

[29] Cohn, J.H.E., Acta Arith., 28 (1975/1976), No.3, 273—275.

[30] Cohn, J.H.E., Math. Scand., 42 (1978), 180—188.

[31] 柯召，孙琦，数学年刊，4 (1981)，491—495。

[32] 戴宗恕，曹珍富，哈尔滨工业大学科研报告，253 (1982)，1页（见“关于丢番图方程 $x^2-Dy^4=1$”一文，哈尔滨工业大学学报将发表）。

[33] Barrucand, P. and Cohn, H., J. Reine Angew. Math., 262/263 (1973), 400—414.

[34] Ljunggren, W., Skr. Norske Vid. Akad. Oslo, I. No. 9 (1942), 53pp. MR6 (1945), 169页.

[35] Ljunggren, W., Avh. Norske Vid. Akad. Oslo, I. No.5 (1942), 27pp.

[36] Cohn, J.H.E., Pacific J. Math. 3 (1972), 631—646.

[37] Mordell, L.J., Acta Arith., 15 (1969), 269—272.

[38] Ljunggren, W., Arch. Math. Naturv., 48 (1946), Nr. 7, 26—29.

[39] Cassels, J.W.S., Proc. London Math. Soc. (3), 14A (1965), 55—57.

[40] Cohn, J.H.E., Pacific J. Math., 37 (1971), 331—335.

[41] Ponnudurai, T., J. London Math. Soc. (2), 10 (1975), 232—240.

[42] 宣体佐，北京师范大学学报（自然科学版），3（1982），27—33。

[43] 曹珍富，哈尔滨工业大学科研报告，253(1982)，13页。

[44] Jeyaratnam, S., Pacific J. Math., 60（1975），No.1, 183—187.

[45] Ljunggren, W., Math. Scand., 21(1967), 149—158.

[46] 柯召，孙琦，四川大学学报（自然科学版），4（1979），1—3。

[47] 姚琦，山东大学学报（自然科学版），2(1983)，16—19。

[48] Velupillai, M., Bull. Cal. Math. Soc., 68(1976),275—278.

[49] Cohn, J.H.E.,Pacific J. Math., 26(1968), 233—243.

[50] Tzanakis, N., J. Number Theory,17(1983), 144—164.

[51] Tzanakis, N., Acta Arith., 46 (1986), 257—269.

[52] Turk, J.W.M., Products of integers in Short intervals, Econometric Institute, Erasmus University, Rotterdam, Report 8228/M, P.37.

[53] Dickson, L.E., History of the Theory of Numbers, Vol. II. Chelsea Publishing Company, New York, 1952.

[54] Pocklington, H·C., Proc. Camb. Phil. Soc., 17 (1914), 110—118.
[55] Sinha, T.N., Amer. J. Math., 100(1978), 585—590.
[56] 张明志，四川大学学报(自然科学版)，2(1983)，24—31。
[57] 郑德勋，四川大学学报(自然科学版)，3(1986)，10—15。
[58] 郑德勋，科学通报，8 (1987)，571—572。
[59] Sinha, T.N.,Math.Stud.,43(1975),61—64.
[60] Mordell, L.J., Q.J. Math., (2)18 (1967), 1—6.
[61] Ward, M., Proc. Nat. Acad. Sci., 31 (1945), 125—127.
[62] Ward, M., Duke Math. J., 15 (1948), 827—837.
[63] Lander,L.J.,Parkin, T.R. and Selfridge, J.L., Math. Comp., 21 (1967), 446—453.
[64] Guy, R.K., Unsolved problems in number theory, Section D1, Springer, New York, 1981.
[65] 郑格于，初等数学论丛，6 (1983)，56—70。
[66] Norrie, R., Univ. of St. Andrews 500th Anniv. Mem. Vol., Edinburgh, 1911, 89.
[67] Ljunggren,W., Norske Vid. Selsk. Forhdl., 24 (1952), 82—84.

第八章　高次丢番图方程

本章介绍各种类型的高次丢番图方程的解法和主要结果。

§1　丢番图方程$x^{2n}-Dy^2=1$和$x^2-Dy^{2n}=1$

丢番图方程

$$x^{2n}-Dy^2=1,\ n>1,\ D>0\text{ 且不是平方数} \tag{1}$$

的可解性，在$n=2$时已经有过大量的工作（参阅第七章§1）。现在我们来研究$n>2$的情形。1986年，曹珍富[1]证明了

定理 1　如果$n>2$，且Pell方程$X^2-DY^2=-1$有整数解，则方程（1）仅在$n=5$，$D=122$时有正整数解$x=3$，$y=22$。

这个定理的证明用到了方程

$$x^p+1=2y^2,\ p\text{是素数}>3 \tag{2}$$

和

$$x^p-1=2y^2,\ p\text{是素数}>3 \tag{3}$$

的结果。在$p=3$时，（2）和（3）的全部解已在第六章的§2中给出，即方程$x^3+1=2y^2$仅有整数解$(x,\ y)=(-1,\ 0)$，$(1,\ \pm1)$和$(23,\ \pm78)$，而方程$x^3-1=2y^2$仅有整数解$(x,\ y)=(1,\ 0)$。

Nagell[2]和曹珍富[3]分别用不同的方法给出了方程(3)

的全部解，证明了（3）仅有正整数解$p=5$，$x=3$，$y=11$。对方程（2），我们有[3]

定理 2 如果方程（2）有正整数解，则除$x=y=1$外必有 $2p|y$。

证 由方程（2）得

$$(x+1)\left(\frac{x^p+1}{x+1}\right)=2y^2,$$

由于$\left(x+1, \frac{x^p+1}{x+1}\right)=1$ 或 p，故上式给出

$$x+1=2y_1^2, \quad \frac{x^p+1}{x+1}=y_2^2, \quad y=y_1y_2, \tag{4}$$

或

$$x+1=2py_1^2, \quad \frac{x^p+1}{x+1}=py_2^2, \quad y=py_1y_2。 \tag{5}$$

由本章后面的§3知，（4）的第二式给出$x=1$，$y_2=1$，故给出（2）有正整数解 $x=1$，$y=1$。

对于（5）式，此时已有$p|y$，故只需证明$2|y$。为此，设$2\nmid y$，则由（5）式的第一式给出$x\equiv1 \pmod 4$，这就有$(-x)+1\equiv0 \pmod 4$，于是由第二章 §5 的例 2 知方程$\frac{(x)^p-1}{(-x)-1}=py_2^2$无解，这就证明（5）的中间一式不成立。于是有$2|y$，从而 $2p|y$。证毕。

现在我们给出定理 1 的证明。设$X^2-DY^2=-1$ 的基本解为$\delta=X_0+Y_0\sqrt{D}$，则由第五章§3可知，方程(1)给出

$$x^n+y\sqrt{D}=\delta^{2m}, \quad m>0。$$

令$\overline{\delta}=X_0-Y_0\sqrt{D}$，$\delta\overline{\delta}=-1$，则上式给出

$$x^n=\frac{\delta^{2m}+\overline{\delta}^{2m}}{2}=2\left(\frac{\delta^m+\overline{\delta}^m}{2}\right)^2-(-1)^m。 \tag{5'}$$

由 $n>2$ 知必有 $4|n$ 或 $p|n$，p 为奇素数。在 $4|n$ 时，可设 $n=4r$，$r>0$，则（5′）式为

$$(x^r)^4-2\left(\frac{\delta^m+\bar{\delta}^m}{2}\right)^2=(-1)^{m+1},$$

此由方程 $x^4-2y^2=\pm1$ 的结果知，仅给出 $x^r=1$，这由(1)知 $y=0$，不是（1）的正整数解。

在 $p|n$ 时，可设 $n=pr$，$r>0$，则（5′）式化为

$$(x^r)^p+(-1)^m=2\left(\frac{\delta^m+\bar{\delta}^m}{2}\right)^2。\qquad(6)$$

在 $2|m$ 时，由定理 2 知 $2p\left|\frac{\delta^m+\bar{\delta}^m}{2}\right.$，但由 $2|m$，设 $m=2l$ 得

$$\frac{\delta^{2l}+\bar{\delta}^{2l}}{2}=2\left(\frac{\delta^l+\bar{\delta}^l}{2}\right)^2-(-1)^l$$

为奇数，故（6）给出 $2\nmid m$，即有

$$(x^r)^p-1=2\left(\frac{\delta^m+\bar{\delta}^m}{2}\right)^2。$$

此由关于方程(3)的结果知，仅有 $p=5$，$x^r=3$，$\frac{\delta^m+\bar{\delta}^m}{2}=11$。由此给出方程（1）仅有正整数解 $n=5$，$D=122$，$x=3$，$y=22$。证毕。

利用这种方法，曹珍富[3],[4]还证明了以下一系列结果。

定理 3 设 $\varepsilon=u_0+v_0\sqrt{D}$ 为Pell方程 $u^2-Dv^2=1$ 的基本解，则方程（1）的正整数解不满足

$$x^n+y\sqrt{D}=\varepsilon^{4m},\ n>2,\ m>0。$$

定理 4 设 $n>2$，$D\equiv0\pmod 2$ 且方程 $u^2-Dv^2=2\eta$（$\eta=\pm1$）有整数解，则方程（1）无正整数解。

这个定理的证明用到了方程 $x^n\pm1=y^2$ 的结果（本

章§3）。

推论 1 设$n>2$，$D=2p$，$p\equiv 3 \pmod 4$是素数，则方程（1）无正整数解。

推论 2 设$n>2$，$D=2(2t^2\pm 1)$，$t\in Z$，则方程（1）无正整数解。

对$n=3$，我们有[4]

定理 5 设方程$u^2-Dv^2=2\eta$（$\eta=\pm 1$）有整数解，则方程$x^6-Dy^2=1$除开$D=7$，$x=2$，$y=3$外，无其它的正整数解。

定理 6 设$D\equiv 3 \pmod 8$且Pell方程$u^2-Dv^2=1$的基本解$\varepsilon=u_0+v_0\sqrt{D}$满足$2|u_0$，则方程$x^6-Dy^2=1$除开$D=6083$（$=7\cdot 11\cdot 79$），$x=23$，$y=156$外，无其它的正整数解。

显然，在研究方程（1）的过程中，方程（2）起了决定性作用。曹珍富[5]提出了如下猜想：丢番图方程（2）在$p>3$时仅有正整数解$x=y=1$。这个猜想如果得到证明，那么定理3—6都将得到很大的改进。进而可能证明：在$n>2$时方程(1)的正整数解x，y满足$x^n+y\sqrt{D}=\varepsilon$，这里$\varepsilon$为Pell方程$u^2-Dv^2=1$的基本解。

Tartakowski[6]对于丢番图方程

$$x^{2n}-Dy^{2n}=1,\ n>2,\ D>0\text{且不是平方数},\qquad (7)$$

证明了

定理 7 设Pell方程$u^2-Dv^2=1$的基本解为ε，则(7)的正整数解x，y满足

$$x^n+y^n\sqrt{D}=\varepsilon \text{ 或 } \varepsilon^2,$$

且ε^2仅出现有限次。

他在方程$X^2-DY^2=-1$有整数解时证明了(7)仅有

解 $y=0$。这一结果包含在定理1中。此外，对定理7中ε^2出现的次数可进一步证明为1，且ε^2出现时必有$D\equiv 7 \pmod 8$。如果$2|n$，则ε^2不出现。

对于比（7）更为一般的方程

$$x^{2n}-Dy^{2m}=1，D>0\text{且不为平方数}，n>1, m>1，\quad (8)$$

曹珍富[4]还证明了

定理 8 设方程$u^2-Dv^2=2\eta$（$\eta=\pm 1$）有整数解，则方程(8)无整数解。

定理 9 设$D\equiv 3$ (mod8) 且Pell方程 $u^2-Dv^2=1$ 的基本解$u_0+v_0\sqrt{D}$满足$2|u_0$，则在$m>2$时，方程(8)无正整数解。

Ljunggren[7] 考虑了丢番图方程

$$x^2-Dy^{2n}=1，n>2，D>0\text{且不是平方数}\qquad (9)$$

的解，他用Siegel[8] 的一个结果和定理7证明了

定理10 设$n>3$，$D+1$ 不是平方数，则方程(9) 最多有两组正整数解 x，y 。如果$n=3$，则对所有D，方程(9)都最多有两组正整数解。

对于 $D+1$ 是一个平方数，Ljunggren 证明：如果D超过一个仅取决于n的某个界限，则方程(9)也最多有两个正整数解。

曹珍富[9]利用方程（1）的一个结果（定理1)，证明了

定理11 设$D\equiv 2$，5 (mod8)，且Pell方程$X^2-DY^2=-1$有整数解，则方程(9)无正整数解。

证 设 $\delta=X_0+Y_0\sqrt{D}$是Pell方程$X^2-DY^2=-1$的基本解，如果方程(9)有正整数解 x，y，则有

$$x+y^n\sqrt{D}=\delta^{2m}，m>0。$$

令$\overline{\delta}$满足 $\delta\overline{\delta}=-1$ ，则上式给出

$$y^n=\frac{\delta^{2m}-\bar{\delta}^{2m}}{2\sqrt{D}}=2\left(\frac{\delta^m+\bar{\delta}^m}{2}\right)\left(\frac{\delta^m-\bar{\delta}^m}{2\sqrt{D}}\right)。\tag{10}$$

因为

$$\left(\frac{\delta^m+\bar{\delta}^m}{2}\right)^2-D\left(\frac{\delta^m-\bar{\delta}^m}{2\sqrt{D}}\right)^2=(-1)^m,$$

故

$$\left(\frac{\delta^m+\bar{\delta}^m}{2},\ \frac{\delta^m-\bar{\delta}^m}{2\sqrt{D}}\right)=1。$$ 所以(10)给出

$$\frac{\delta^m+\bar{\delta}^m}{2}=2^{n-1}y_1^n,\quad \frac{\delta^m-\bar{\delta}^m}{2\sqrt{D}}=y_2^n,\quad y=2y_1y_2,\tag{11}$$

或

$$\frac{\delta^m+\bar{\delta}^m}{2}=y_1^n,\quad \frac{\delta^m-\bar{\delta}^m}{2\sqrt{D}}=2^{n-1}y_2^n,\quad y=2y_1y_2。\tag{12}$$

由(11)式得出

$$(2^{n-1}y_1^n)^2-Dy_2^{2n}=(-1)^m,$$

此在$D\equiv2(\mathrm{mod}8)$时显然不成立，而在$D\equiv5$ (mod8) 时，对上式取模 8 得$-5\equiv(-1)^m$ (mod 8)，此不可能。现由 (12) 式得

$$y_1^{2n}-D(2^{n-1}y_2^n)^2=(-1)^m,$$

取模4知 $2|m$，故由定理1知，此时也不可能。这就证明了定理11。证毕。

由定理11可知，设$D=2$，p或$2p$，这里$p\equiv5(\mathrm{mod}8)$是素数，则方程（9）无正整数解；设$D=(2k+1)^2+1$，或$D=(4k+2)^2+1$，$k\in Z$，则方程 (9) 无正整数解。

由方程（1）和 (9) 的结果可以推出$\binom{n}{2}$不是一个$2k$次幂 ($k>1$) 。这是Erdös 关于组合数$\binom{m}{n}$猜想的偶指数情形的最后解决[10]。同时，由于Pell方程$x^2-Dy^2=1$的解x_n和y_n各构成一个Pell序列

$$x_0=1,\quad x_1=a,\quad x_{n+2}=2ax_{n+1}-x_n, \tag{13}$$

和

$$y_0=0,\quad y_1=b,\quad y_{n+2}=2ay_{n+1}-y_n, \tag{14}$$

这里 $\varepsilon=a+b\sqrt{D}$是 Pell方程$x^2-Dy^2=1$的基本解。故利用定理 1 和定理11可给出Pell序列（13）和（14）在某些条件下没有k（>2）次方数，例如有

推论 3[3]　设$a=2u^2+1$，则Pell序列（13）中除$x_0=1$和$x_1=2\cdot 11^2+1=3^5$外，没有其他的$k>2$ 次幂。

推论 4[10]　设$a=2u^2+1, b=2uv$，这里$u^2-Dv^2=-1$，且$D\equiv 2$，5（mod8），则Pell序列（14）中没有 $k>2$ 次幂（除 $y_0=0$）。

现取$D=5$，则$u=2$，$v=1$，于是$a=9$，$b=4$，Pell 序列（14）即为

$$y_0=0,\quad y_1=4,\quad y_{n+2}=18y_{n+1}-y_n, \tag{15}$$

由推论4的结论知，序列(15）中除 $y_0=0$外没有一个$k>2$次幂。

最后指出，在D的某些更强的条件下，可以改进前面的某些定理，例如，王笃正和曹珍富[11]证明了在$D\not\equiv 3(\text{mod}4)$时，方程（1）的正整数解 x，y 不满足

$$x^n+y\sqrt{D}=\varepsilon^{2m},\quad n>2,\quad m>0,$$

这里 $\varepsilon=u_0+v_0\sqrt{D}$为Pell方程$u^2-Dv^2=1$ 的基本解。在$D\equiv 3$（mod4）时还可从如下的一个结果中得到一些补充。

定理12　设Pell 方程 $u^2-Dv^2=1$ 的基本解 $\varepsilon=u_0+v_0\sqrt{D}$满足$2\nmid u_0$，则方程（1）的正整数解 x，y 不满足

$$x^n+y\sqrt{D}=\varepsilon^{2m},\quad n>2,\quad m>0。 \tag{16}$$

推论 5　设$D=pq$，p，q是素数，且$p\equiv 5$（mod 8），

$q\equiv 7 \pmod 8$，$\left(\frac{q}{p}\right)=1$，则Pell方程$u^2-Dv^2=1$的基本解 $\varepsilon=u_0+v_0\sqrt{D}$满足$2\nmid u_0$，故方程（1）的正整数解不满足（16）式。

§2 丢番图方程$ax^2+bx+c=dy^n$

对于丢番图方程

$$ax^2+bx+c=dy^n,\quad n\geqslant 3,\quad ad\neq 0, \tag{1}$$

这里a，b，c，d均是给定整数，一个已知的结果是由 Landau 和Ostrowski[12]以及 Thue[13] 给出的。

定理 1 如果$b^2-4ac\neq 0$，则方程（1）最多只有有限个整数解 x，y。

Ljunggren 大力地研究了方程（1）的一些特殊情形，他[14]证明了

定理 2 设二次域$Q(\sqrt{-D})$的类数h不被n整除，则丢番图方程$1+Dx^2=2y^n$（当$D\equiv 1 \pmod 4$）和$1+Dx^2=4y^n$（当$D\equiv 3 \pmod 4$）均没有满足$y>1$的整数解。

由此推出，方程$1+x^2=2y^n$，$n\geqslant 3$仅有正整数解$x=1$，$y=1$，以及方程$1+3x^2=4y^n$，$n\geqslant 3$仅有正整数解$x=1$，$y=1$，等等。

对于丢番图方程

$$x^2+D=y^n,\qquad n>1, \tag{2}$$

1944年，Ljunggren[15] 利用代数数论方法证明了

定理 3 设$D\equiv 1 \pmod 4$，$D>0$ 无平方因子。如果$D-1=2^{2k+1}D_1$，$2\nmid D_1$，$k\geqslant 0$，且n不整除$Q(\sqrt{-D})$的类数，$2\nmid n$，则方程（2）无整数解。

当$D=p^2$，p是一个素数时，方程（2）化为

$$x^2+p^2=y^n,\quad n>1, \tag{3}$$

这时把 x，y，n 都看成变元来研究方程（3）的解数，Ljunggren[16] 证明了

定理 4 设$D=p^2$，p是素数且$p^2-1=2^{2k+1}l$，$2\nmid l$，$k\geqslant 0$，则方程（3）最多只有有限个正整数解x，y和n。

1985年，Kawamoto[17]发现Ljunggren关于定理 4 的证明有误，因而他重新给出了一个完全的证明。

首先，在$Q(\sqrt{-1})$中分解（3）式（注意$D=p^2$），容易证明[16]：

1） 设$2\nmid n$且方程（3）有解，则$y=a^2+1$或a^2+p^2，$a\in Z$。

2） 设$n=rs$，r，s 均是奇素数且方程（3）有解，则$y=a^2+1$，$a\in Z$。如果$r\neq s$，则方程（3）没有解。

3） 设$2\nmid n$，$p^2-1=2^{2k+1}l$，$2\nmid l$，$k\geqslant 0$，则$y=a^2+p^2$，$a\in Z$ 时不满足（3）式。

其次，我们可以证明[17]

4） 设$n=r^2$，r 是奇素数，且 $p^2-1=2^{2k+1}l$，$2\nmid l$，$k\geqslant 0$，则 $y=a^2+1$不满足（3）。

证 若 $y=a^2+1$满足（3），则有

$$x^2+p^2=[(a^2+1)^r]^r,$$

故得出

$$x+pi=[(a\pm i)^r]^r=(c+di)^r,\quad c+di=(a\pm i)^r。\tag{4}$$

从（4）的第一式知$d\mid p$，故$d=\pm 1$或$\pm p$。如果$d=\pm 1$，则（4）的后一式给出$c^2+1=(a^2+1)^r$，这是方程$x^2+1=y^r$（r 为奇素数）的特例（见 §3），易知这不可能。于是$d=\pm p$，从而

$$x^2+p^2=(c^2+p^2)^r。$$

但这由3)知也不可能。这就证明了4)。

由1)～4)容易推出定理4。

当D取一些具体数值时，我们可以给出（2）的全部解。例如，1943年，Ljunggren[18]第一个给出了方程 $x^2+2=y^n$（$n>1$）的全部解。后来，Nagell[19][20]在1955年前后又给出了方程$x^2+8=y^n$（$n>1$）的全部解。1977年，Brown[21]在$m\geq3$为奇数，n为奇素数且$(a)2\nmid y$，$n\not\equiv-1(\mathrm{mod}\,8)$或$(b)$ $2|y$，$n>\frac{m-1}{2}$，$n\neq m$时解决了如下方程

$$x^2+2^m=y^n,\quad n>2。\tag{5}$$

1983年，Toyoizumi[22]解决了方程（5）当$y=3$时的特殊情形。1986年，曹珍富[23]彻底解决了方程（5），证明了

定理 5 方程（5）的全部正整数解为$(m, n, x, y)=(6s+1, 3, 2^{3s}\cdot5, 2^{2s}\cdot3)$，$(6s+2, 3, 2^{3s}\cdot11, 2^{2s}\cdot5)$，$(4s+5, 4, 2^{2s}\cdot7, 2^s\cdot3)$，$(10s+5, 5, 2^{5s+3}\cdot11, 2^{2s+1}\cdot3)$和$((2s+3)(2t+1)-1, 2s+3, 2^{(2s+3)(2t+1)-1}, 2^{2t+1})$，其中$s$，$t$为任意非负整数。

这个定理的证明，主要困难在于解决$2\nmid y$的情形。此时我们分成$y\equiv3$（mod4），$y\equiv5$（mod8）和$y\equiv1$（mod 8）三部分来讨论：

1）$y\equiv3$（mod 4）时，如果$m=1$，则由$x^2+2=y^n$（$n>1$）仅有正整数解$x=5$，$y=3$，$n=3$知，（5）仅有解$(m, n, x, y)=(1, 3, 5, 3)$。如果$m>1$，则对（5）取模4知$2|n$，故用分解因子法易知，仅有$(m, n, x, y)=(5, 4, 7, 3)$。

2）$y\equiv5$（mod8）时，如果$m\geq3$，则（5）给出$2|n$，

故易知（5）仅给出（m，n，x，y）=（4，2，3，5）。如果$m<3$，则$m=1$或2。易知$m=1$不可能，所以$m=2$，方程（5）化为

$$x^2+4=y^n,\quad 2\nmid n。$$

由Gauss整数的性质知$y=k^2+4$。利用Ljunggren的一个定理（见第七章§3）知$n\equiv 3\pmod 4$，$k\equiv\pm 1\pmod 5$，于是利用Pell方程的解法知，仅有$k=\pm 1$，给出（5）此时仅有解（m，n，x，y，）=（2，3，11，5）。

3）$y\equiv 1\pmod 8$时，如果$2|n$，易知不可能。如果$2\nmid n$，则在$2|m$时用Gauss整数的性质可证也不可能；而且在$2\nmid m$时，在二次域$Q(\sqrt{-2})$中讨论（5），易知也不可能。

在$2|y$时，定理5的证明需用方程

$$x^2+1=2y^n,\quad n>2 \tag{6}$$

$$2x^2+1=y^n,\quad n>2, \tag{7}$$

和

$$x^2+1=y^n,\quad n>1 \tag{8}$$

的结果。方程（7）在§1中已经介绍过，方程(8)是Catalan猜想的特例，早已由Lebesgue[4]解决（一个证明见第二章§4）。而方程（6）是定理2的特例。实际上，Störmer[25]也曾解决了方程（6）。

Brown[21]还讨论了方程$x^2+3^{2m+1}=y^p$，$3x^2+2^{2m}=y^p$以及$2x^2+3^{2m}=y^p$（这里$m\geqslant 0$，p为奇素数）的解。

Nagell[2?]对于方程

$$x^2+8D=y^n,\quad n\geqslant 3, \tag{9}$$

这里D无平方因子，$2\nmid D>0$，证明了若干定理，例如他证明了

定理 6 设$n>3$是奇数，$Q(\sqrt{-2D})$的类数不被n整除。如果$D\equiv 1 \pmod 3$，则方程（9）没有整数解。

定理 7 设$n=p^f$，$f\geqslant 1$，$p\equiv \pm 1 \pmod 8$为奇素数，且$Q(\sqrt{-2D})$的类数不被n整除，则方程（9）最多有一个正整数解x，y。

Brown[26]还讨论了方程（2）当$D=3$，5的情形，例如他用代数数论的基本知识证明了

定理 8 方程$x^2+3=y^n$，$n>2$没有解。

方程$x^2+5=y^n$，$n>2$早已由Nagell[27]证明是没有解的。当$D\equiv 1$或$2 \pmod 4$，$D>0$无平方因子时，Nagell还给出寻求方程（2）的全部整数解的方法。

Ljunggren[28]对于丢番图方程

$$x^2+4D=y^n,\quad (y,\ 2)=1 \tag{10}$$

证得

定理 9 设$n=q$是奇素数，$D>1$，$2\nmid D$且D无平方因子>1。如果$Q(\sqrt{-D})$的类数不被奇素数q整除，则在$q\not\equiv 3 \pmod 8$时，方程（10）无整数解；而在$q\equiv 3 \pmod 8$时，对给定D，方程（10）最多只有有限多组解x，y和素数q，且这些解可以有效计算。

例如Ljunggren给出两个例子：

例 1 丢番图方程

$$x^2+28=y^z,\quad z>1 \tag{11}$$

在第六章已解决了$z=3$的情形。现设$z>3$，则有[28]方程(11)在$2\nmid yz$时无解。

例 2 丢番图方程

$$x^2+12=y^z,\quad z>1$$

在 $2\nmid z$ 时无解。

对于丢番图方程

$$cx^2+D=y^n,\quad n>1, \tag{12}$$

设 c，D和 n 都是正奇数，$D>1$ 和 cD无平方因子>1，$Q(\sqrt{-cD})$ 的理想类数为h，且令$D+(-1)^{\frac{D+1}{2}}=2^m\cdot D_1$，$2\nmid D_1$，则 Ljunggren[29][30] 证明了以下三个定理：

定理10 如果$h\not\equiv 0\pmod{n}$，$m\equiv 1\pmod{2}$ 且$cD\equiv 1\pmod{4}$ 或$cD\equiv 3\pmod{8}$，$n\not\equiv 0\pmod{3}$，则方程(12)没有整数解 x，y。

定理11 设 $n=q>3$ 是素数，$cD\not\equiv 7\pmod{8}$。如果 $h\not\equiv 0\pmod{q}$，$m\equiv 0\pmod{2}$ 且$q\not\equiv cD_1\pmod{8}$，则方程（12）无整数解 x，y。

定理12 如果$D\equiv 1\pmod{4}$，$cD\not\equiv 7\pmod{8}$且 $2|m$，则对给定的 c，D，在 $cD_1\equiv 5\pmod{8}$ 或 $c=1$，$D_1\equiv 3\pmod{8}$ 时，方程（12）最多只有有限个正整数解x，y和 q（素数）。

1964年，Ljunggren[28] 进一步证明了

定理13 设$n=p^f$，$p>3$是素数，且$h\not\equiv 0\pmod{n}$。如果 $p\not\equiv 3c(-1)^{\frac{c-1}{2}}\pmod{8}$ 或$D\equiv 0\pmod{p}$，则丢番图方程

$$cx^2+4D=y^n,\quad n>1,\quad 2\nmid y, \tag{13}$$

没有整数解。

证 由于两个主理想数$[cx+2\sqrt{-cD}]$ 与 $[cx-2\sqrt{-cD}]$的最大公理想因子为$[c,\sqrt{-cD}]$，$[c]=[c,\sqrt{-cD}]^2$且易知 $(x,y)=1$，故（13）给出

$$[cx+2\sqrt{-cD}]=[c,\sqrt{-cD}]\cdot A^{p^f},$$

这里A是域$Q(\sqrt{-cD})$中的一个理想数。所以

$$[cx+2\sqrt{-cD}]^2=[c]\cdot A_1^{p^f}(A_1=A^2),\quad (14)$$

如果类数h被p^e（$0\leqslant e<f$）整除，但不被p^{e+1}整除，则存在两个有理整数α，β使得

$$\alpha p^f-\beta h=p^e。$$

因此由（14）式，我们有

$$A_1^{p^e}\sim A_1^{\alpha p^f}\sim[1]。$$

于是有理想数方程

$$[cx+2\sqrt{-cD}]^2=[c]\cdot\left[\frac{u+v\sqrt{-cD}}{2}\right]^{p^{f-e}},\quad (15)$$

这里u,v是有理整数，且$u\equiv v\pmod 2$。因为$p>3$，$Q(\sqrt{-cD})$中的所有单位数是p次幂，故（15）式给出

$$(cx+2\sqrt{-cD})^2=c\left(\frac{u_1+v_1\sqrt{-cD}}{2}\right)^p,$$

$$u_1\equiv v_1\pmod 2。\quad (16)$$

由于可写 $\dfrac{u_1+v_1\sqrt{-cD}}{2}=\left(\dfrac{a_1\sqrt{c}+b_1\sqrt{-D}}{2}\right)^2$，$a_1\equiv b_1\pmod 2$，故（16）式给出

$$x\sqrt{c}+2\sqrt{-D}=\left(\frac{a_2\sqrt{c}+b_2\sqrt{-D}}{2}\right)^p,$$

$$a_2\equiv b_2\pmod 2。\quad (17)$$

比较$\sqrt{-D}$的系数，（17）式给出

$$2^{p+1}=\sum_{r=0}^{\frac{p-1}{2}}\binom{p}{2r+1}a_2^{p-1-2r}b_2^{2r+1}c^{\frac{p-1}{2}-r}(-D)^r,\quad (18)$$

此给出$b_2\mid 2^{p+1}$，故$b_2=\pm 2^s$，$0\leqslant s\leqslant p+1$。现对（18）取模$p$得

$$b_2^2(-D)^{\frac{p-1}{2}} \equiv 2^{p+1} \pmod p ,$$

此即

$$b_2\left(\frac{-D}{p}\right) \equiv 4 \pmod p ,$$

$$b_2 \equiv \pm 4 \pmod p 。$$

由于$b_2 = \pm 2^s$，$0 \leqslant s \leqslant p+1$，故在$p>5$时，上式给出$s>0$，于是$a_2$，$b_2$均是偶数，（17）给出

$$x\sqrt{c} + 2\sqrt{-D} = (a\sqrt{c} + b\sqrt{-D})^p 。\quad (19)$$

如果$p=5$，则$b_2 = \pm 1$，由(18)得出 $D^2 \pm 16 = 5\left(\frac{ca_2^2 - D}{2}\right)^2$，对此取模8知不可能。

利用一些同余技巧，从（19）可以获得定理13的证明。用类似的方法，还可证明

定理14 如果 $h \not\equiv 0 \pmod n$，$D \equiv (-1)^{\frac{c-1}{2}} \pmod 3$，且下列条件的一个成立：

1） $c \equiv 0 \pmod 3$；

2） $c \equiv \pm 1 \pmod 8$；

3） $c \equiv \pm 3 \pmod 8$ 且 $c \equiv (-1)^{\frac{c-1}{2}} \pmod 3$ ，

则方程（13）没有整数解x，y（在$cD \equiv 3 \pmod 8$ 时还要求$n \not\equiv 0 \pmod 3$)）

对于一个具体的方程$3x^2 + 28 = y^n$，$n \geqslant 3$，用以上方法可以证明在$n>3$时无整数解。

对于丢番图方程

$$x^2 + D = 4y^n,\ n>2,\ x>0,\ y>0, \quad (20)$$

这里$D \equiv 3 \pmod 4$ 是一个无大于 1 的平方因子的正整数，曾经有过很多工作。例如$D=3$，$x=2z+1$，（20）化为

$$z^2+z+1=y^n,\ n>2,\ z\geqslant 0,\ y>0, \tag{21}$$

Nagell[31]证明了在$3\nmid n$时方程（21）没有$y\neq 1$的整数解。他同时还证明了方程

$$z^2+z+1=3y^n,\ n>2,\ z>0,\ y>0$$

在$z>1$时没有解。Ljunggren[32]给出方程（21）在$n=3$时仅有解$y=1$和$y=7$。Persson[33]对于方程

$$z^2+z+\frac{D+1}{4}=y^n,\ n>2,\ D>3, \tag{22}$$

这里$D\equiv 3\pmod 4$，证明了

定理15 设$n=p$是给定的奇素数，$Q(\sqrt{-D})$的类数h满足$p\nmid h$，则仅有有限个D使得方程(22)有解x，y，并且方程（22）的整数解$y<\frac{1}{4}D\operatorname{cosec}^2\frac{\pi}{p}+1$。对给定的$D$和$p$，方程（22）最多有$\frac{p-1}{2}$个解$y$。

这个定理的后一部分在1957年又被Stolt[34]加以改进，得到如下的

定理16 设$n=p$是给定的奇素数，$Q(\sqrt{-D})$的类数h满足$p\nmid h$，则方程（22）除开$D\equiv 3\pmod 8$，$p\equiv 1\pmod 6$最多有三个解y外，其他情形最多有一个解y。

1971年，Ljunggren[35]进一步研究了$D\equiv 7\pmod 8$的情形，设h是二次域$Q(\sqrt{-D})$的类数，则有

定理17 设n是奇素数，$D\equiv 7\pmod{24}$，且$n\equiv 3\pmod 8$或$n\equiv 5\pmod 8$，$D-4=3^{2m+1}D_1$，$D_1\not\equiv 0\pmod 3$，则在$(n,h)=1$时，方程（20）最多仅有有限组正整数x，y和奇素数n的解。

定理18 设$D\equiv 15(\bmod 72)$，$(n, h)=1$，n是奇素数，则方程（20）最多只有有限组正整数x，y和奇素数n的解。

1972年，Ljunggren[36]又在$D\equiv 3\ (\bmod 8)$时证明了两个新定理。

定理19 设$n\not\equiv\pm 1\ (\bmod\ 24)$是奇素数，$(n, h)=1$，则方程（20）仅有有限组正整数$x$，$y$和$n$的解。

定理20 设$n\not\equiv -1(\bmod 24)$是奇素数，$D\equiv 51(\bmod 72)$，则方程（20）仅有有限组正整数x，y和n的解。

定理17～20中的解如果存在，都可以有效地定出（利用Cassels 定理，见第五章§7）。这些定理的证明用到了代数数论方法和递推序列的技巧。例如在$(h, n)=1$时，设$\lambda=\dfrac{a+\sqrt{-D}}{2}$，$\bar{\lambda}=\dfrac{a-\sqrt{-D}}{2}$，$a>0$，则方程(20)给出

$$\frac{\lambda^n-\bar{\lambda}^n}{\lambda-\bar{\lambda}}=b=\pm 1。$$

令

$$T_m=\frac{\lambda^m-\bar{\lambda}^m}{\lambda-\bar{\lambda}}，\quad S_m=\lambda^m+\bar{\lambda}^m，$$

由 $2\nmid n$ 知

$$T^2_{\frac{n+1}{2}}-\lambda\bar{\lambda}\,T^2_{\frac{n-1}{2}}=b,$$

$$T_{\frac{n+1}{2}}\cdot S_{\frac{n-1}{2}}=b+(\lambda\bar{\lambda})^{\frac{n-1}{2}},$$

$$T_{\frac{n-1}{2}}\cdot S_{\frac{n+1}{2}}=b-(\lambda\bar{\lambda})^{\frac{n-1}{2}},$$

$$T_m=(a^2-\lambda\bar{\lambda})T_{m-2}-a\lambda\bar{\lambda}\,T_{m-3},$$

$$S_m=(a^2-\lambda\bar{\lambda})S_{m-2}-a\lambda\bar{\lambda}\,S_{m-3}。$$

于是利用简单同余法可得出一系列结论。

对于具体的例子，例如方程

$$x^2+11=4y^n\quad，n\text{为奇素数，}$$

在$n\not\equiv\pm1\pmod{24}$时除 $n=5$，$y=3$ 是仅有的解外，无其他的整数解。证明时还需用到其他一些技巧，例如 Skolem 的p-adic方法[37]。

最后，我们来讨论丢番图方程

$$1+Dx^2=y^n,\ n>3\text{是素数} \tag{23}$$

的解。Nagell[27]首先证明了

定理21 设 $D>2$ 无平方因子，$n\nmid h$，这里h为二次域$Q(\sqrt{-D})$的类数，则方程（23）的解满足$2|y$。

1985年，曹珍富[38]证明了$D=7$时方程（23）无解。随后，又[39]一般性地证明了：设D不含 $2mn+1$ 形的素因子，则除$1+2\cdot11^2=3^5$外，方程（23）如有解，必有 $2n|x$，故结合定理21可得[40]

定理22 设$D>2$不含$2mn+1$形素因子，$n\nmid h$，这里h是$Q(\sqrt{-D})$的类数，则方程（23）仅有 $x=0$ 的整数解。

1987年，孙琦[41]给出$D=15$和23时方程（23）仅有$x=0$的整数解的证明。曹珍富[40]给出了在$2<D<100$时方程(23)的全部解，证明了除$D=31$方程（23）仅有正整数解$n=5$，$x=1$，$y=2$外，其他情形均无整数解。

§3 丢番图方程 $ax^m-by^n=c$

丢番图方程

$$ax^m-by^n=c,\ m>1,\ n>1,\ c\neq0 \tag{1}$$

(这里a,b,c是给定整数)的一个简单情形,是著名的Catalan方程

$$x^m-y^n=1,\ m>1,\ n>1。 \tag{2}$$

1842年，Catalan曾猜想：方程（2）仅有正整数解$m=2$，$n=3$，$x=3$，$y=2$。这个猜想的证明可简化为证明

$$x^p-y^q=1,\ p,\ q\text{是素数},\ p\neq q \tag{3}$$

仅有正整数解$p=2$，$q=3$，$x=3$，$y=2$。1850年，Lebesgue[34]证明了$q=2$时Catalan猜想是对的（柯召[42]给出了另一个证明，见第二章§4）。对于$p=2$，经过Nagell，Obláth，Hyyrö，Inkeri和柯召等的努力（参阅[43]），在1962年由柯召[44]最后解决，他证明了在$p=2$，$q>3$时（3）无解（这就是著名的柯召定理）。后来，Chein[45]，Rotkiewicz[46]和曹珍富[47]分别给出了柯召定理的一个简化证明（见第二章§5，§6和§8）。有一个弱型的Catalan问题是：设p，q，r都是素数，则方程组

$$\begin{cases} x^p+1=y^q \\ y^q+1=z^r \end{cases} \tag{4}$$

有$y\neq 0$的解吗？这个问题已由Cassels[48]和柯召[49]分别独立地解决，他们证明了

定理 1 如果方程（3）有解，必有$p\mid y$，$q\mid x$。

由此立即推出方程组（4）无$y\neq 0$的解。

1975年，Tijdeman[50]利用Baker方法（见第三章§4）基本上解决了Catalan猜想，他证明了对方程（2）的任一组解均有$x^m<c$，这里c是一个绝对常数。近来，c还可以具体地定出，例如$c<10^{10^{500}}$。由于这个界太大，因此彻底解决方程（3），尤其仅用初等方法解决方程（3）仍将是有意义的工作。

在方程（1）中，许多人讨论了$m=n$的情形。例如Siegel[51]证明了

定理 2 设a，b，c是正整数，$n\geqslant3$，如果$(ab)^{\frac{n}{2}-1}\geqslant 4c^{2n-2}(n\prod\limits_{p}p^{\frac{1}{n-1}})^{n}$，则不等式

$$|ax^n-by^n|\leqslant c,\ (x,\ y)=1 \tag{5}$$

最多只有一组正整数解 x，y。

显然，如果n是素数，则在$(ab)^{1/2}\geqslant188c^4$时，（5）最多有一组正整数解。

Domar[52]利用Siegel关于定理 2 的证明方法，证明了如下的两个定理。

定理 3 方程

$$|ax^n-by^n|=1,\ n\geqslant5$$

（这里a，b是正整数）最多有两组正整数解。

定理 4 方程

$$|x^n-Dy^n|=1,\ n\geqslant5$$

（这里$D>0$，$D\neq2$且当$n=5$或 6 时$D\neq2^n\pm1$）最多有一组正整数解 x，y。

利用定理2和4可以给出§1中定理 7 的证明[53]。1964年，Hyyrö[54]还证明了一系列结果，这些结果有一半是对二元高次丢番图方程的，例如他证明了

定理 5 设$d\geqslant2$，$n\geqslant5$ 是给定整数，则方程

$$|x^n-d^sy^n|=1$$

（这里$x\geqslant2$，$y\geqslant1$，$0\leqslant s<n$，且对于$n=5$，6 时$x\geqslant3$）最多有一组解 s，x，y。

Skolem[55]利用p-adic 方法证明了

定理 6 丢番图方程$x^5+2y^5=1$仅有解$(x,\ y)=(1,\ 0)$，$(-1,\ 1)$；而丢番图方程$x^5+Dy^5=1$（$D=4$，8，16）仅有 $y=0$ 的解。

利用定理 2 可知，当$D>1250\sqrt[6]{20}$时， 方程 $x^5+Dy^5=1$，$y\neq 0$ 最多有一组解。

Ljunggren[56][57] 证明了一个很有用的定理（参阅第九章）：

定理 7 设a，b，c均是正整数，则当

$$n=2,\quad c=1,\ 2,\ 4,\ 8$$

或

$$n=3,\quad c=1,\ 2,\ 3,\ 4,\ 6$$

时，方程

$$ax^{2n}-by^{2n}=c$$

最多有一组正整数解。

利用定理7，我们[58]可以证明指数丢番图方程

$$3^x+29^y=2^z \tag{6}$$

仅有正整数解$(x,\ y,\ z)=(1,\ 1,\ 5)$。这是因为对(6)取一些正整数模知$x=1$，$y\equiv 1\pmod 6$，$z\equiv 5\pmod 6$。令$y=6y_1+1$，$z=6z_1+5$，且令$X=2^{z_1}$，$Y=29^{y_1}$，则(6)化为

$$32X^6-29Y^6=3。$$

由定理 7 知上式仅有正整数解$(X,\ Y)=(1,\ 1)$，故给出$z_1=y_1=0$，从而得出方程(6)仅有正整数解$(1,\ 1,\ 5)$。

1964年，Baker[59] 对方程（1）的一般情形证明了*

定理 8 如果x，$y\in Z$，x，$y>1$，则最多有9组(m,n)满足（1），且$\max(ax^m,\ by^n)>953c^6$。

Siegel 有一个著名的问题：设$F(x,\ y)=a_0x^n+a_1x^{n-1}y+\cdots+a_ny^n$是不可分的整系数二元多项式，$n\geqslant 3$，

---

* 曹珍富于最近证明了：如果$x,y\in Z$，x，$y>1$，且$c=1,2$，则最多有一组(m,n)满足$2\nmid mn$和(1)式。

则方程$F(x, y)=h$，$(x, y)=1$的解的个数的上界是否仅取决于n和h，而与F无关？我们在第三章§4中给出的上界都与F有关。1983年Evertse[60]给出了Siegel问题的一个肯定回答，他得到的上界是$7^{15((\binom{n}{3})+1)^2}+6\cdot7^{2(\binom{n}{3})(t+1)}$，这里$t$是$h$的素因子个数。最近，Bombieri和Schmidt[61]改进了这个上界到c_1n^{1+t}，这里c_1是绝对常数。如果$n>c_2$，我们把(x, y)与$(-x, -y)$看成是相同的，则方程$|F(x, y)|=h$，$(x, y)=1$的解的个数的上界不超过$215n^{1+t}$。应该指出，Baker曾证明方程$F(x, y)=h>0$的解适合$\max(|x|,|y|)<e^{A+B}$，这里$A=(\log h)^{2n+2}$，$B=(nH)^{(10n)^5}$且H为$F(x, y)$的高。

另一类重要的丢番图方程是

$$\frac{x^n-1}{x-1}=y^m,\quad n\geqslant3,\quad m>1,\quad |x|>1, \tag{7}$$

1920年，Nagell[62]证明了

定理 9 如果$4|n$，则方程（7）仅有整数解$n=4$，$x=7$，$m=2$，$y=\pm20$。

1943年，Ljunggren[63]利用代数数论方法证明了

定理10 如果$m=2$，则方程（7）仅有整数解$n=4$，$x=7$，$y=\pm20$和$n=5$，$x=3$，$y=\pm11$。

定理11 如果$3|n$，则方程（7）仅有解$m=n=3$，$x=18$或-19，$y=7$。

定理12 如果$m=3$，$n\not\equiv-1 \pmod 6$，则方程（1）仅有解$n=3$，$x=18$或-19，$y=7$。

由于在$m=2$时，利用Catalan方程$x^2-1=y^n$ $(n>1)$的结果知，（7）给出$2\nmid n$，于是（7）式化为

$$x\left(x^{\frac{n-1}{2}}\right)^2-(x-1)y^2=1。$$

故利用Pell 方程$X^2-x(x-1)Y^2=1$的全部解可以给出定理10的一个简短的初等证明。柯召[64]曾用不等式法证明了：在$m=2$，$2\nmid n$，$|x|>2^{n-2}$时，方程（7）无整数解。

由于对有限群研究的需要，Edgar[65]提出了如下问题：除开$\frac{3^5-1}{3-1}=11^2$外，方程

$$\frac{q^x-1}{q-1}=p^y,\quad x\geqslant 5,\quad y\geqslant 2,\quad p,\ q\text{是素数} \qquad (8)$$

是否存在另外的解？

曹珍富[66]给出了（8）有解的充要条件，证明了

定理13 设$D=p(q-1)$，则方程（8）有$2\nmid y$的解的充要条件是方程$x^2+Dy^2=q^z$有解$x>0$，$y>0$，$z>0$且$x_1=1$，$y_1=p^{\frac{y-1}{2}}$，$z_1=x$。这里x_1，y_1，z_1为满足$x_1^2+Dy_1^2=q^{z_1}$的$x_1>0$，$y_1>0$使z_1为最小的正整数。

由此可推出，对给定的p，q，方程（8）最多有一组解x，y。这个定理的证明，用到了第三章§1的例5。曹珍富还定出了（8）的解x，y的上界，例如$x<\sqrt{pq(q-1)}\cdot\frac{\log(pq(q-1))}{\log q}$。

1972年，Inkeri[67]考虑了更一般的方程

$$a\frac{x^n-1}{x-1}=y^m,\quad n\geqslant 3,\quad m>1 \qquad (8)$$

的解，在$1<a<x\leqslant 10$时，他给出了方程（8）的全部解是$n=a=4$，$x=7$，$m=2$，$y=40$。

1986年，Shorey[68][69]证明了，如果$w(n)>m-2$，$w(n)$

表n的不同素因子的个数，则方程（7）仅有有限组解。如果x是一个m次幂，则x，y，m，n是可以有效计算的。

Shorey[70]还考虑把Baker关于方程（1）的结果（定理8）应用于丢番图方程

$$a\frac{x^m-1}{x-1}=b\frac{y^n-1}{y-1},\quad x>1,y>1,\ m>1,\ n>1 \qquad (9)$$

上。令$A=a(y-1)$，$B=b(x-1)$，$c=a(y-1)-b(x-1)$，则（9）化为

$$Ax^m-By^n=c,$$

由定理8知，对给定的a，b，x，y，方程（9）最多只有9组解（m，n），且$\max(Ax^m, By^n)>953c^6$，故得

定理14 设a，b，x，$y\in Z$，$x^m\neq y^n$，则最多有9组（m,n）满足方程(9)，且$\max(a(y-1)x^m, b(x-1)y^n)>953(a(y-1)-b(x-1))^6$。

最后，Shorey[71][72]研究了丢番图方程

$$ax^m+by^m=ax^n+by^n \qquad (10)$$

的解，证明了

定理15 设a，b，x，y均是非零整数，$|x|\neq|y|$，$(a, y)=1$，$(b, x)=1$，且m，n是不同的非负整数，则存在一个仅与a，b有关的有效常数$c>0$，使得方程（10）推出$\max(m, n)<c$。

不妨设$(a,b)=1$，$m>n$且$|x|>|y|>0$，$ax^m+by^m\neq0$。令$R=\max(|a|, |b|, 2)$，c_1，c_2，…表仅与a，b有关的可计算正常数，则Shorey证明了由（10）推出：

1） $\log R\leqslant c_1(\log|x|+\log(m-n))$；

2） $m-n\leqslant c_2\log m$；

3） 如果$|y|\leqslant\frac{2}{3}|x|$，则$m\leqslant c_3\log|x|$；

4) 令$g=(|x|, |y|)$, $\theta=(\log m)^{-2}$, 则

$$g\leqslant|x|^{1-\theta}。$$

由2)和4)可以证明定理15。改写方程（10）为

$$a\left(\frac{x}{g}\right)^n(x^{m-n}-1)=b\left(\frac{y}{g}\right)^n(1-y^{m-n}),$$

由4）及（b, x）$=1$ 知

$$|x|^{n\theta}\leqslant\left(\frac{|x|}{g}\right)^n\leqslant|1-y^{m-n}|\leqslant2|x|^{m-n},$$

故由2)及上式（注意$\theta=(\log m)^{-2}$）可得

$$n\leqslant c_4(\log m)^3。$$

由2)知，上式给出$m\leqslant c_5(\log m)^3$，由此知 $m<c$。

Shorey[72] 还研究了递推序列

$$u_m=ru_{m-1}+su_{m-2},\ m=2,\ 3,\ \cdots$$

的解 $u_m=a\alpha^m+b\beta^m$ （$m=0$, 1, 2, $\cdots$）所满足的方程。这里u_0, u_1给定，$r^2+4s\neq0$, α, β是 $x^2-rx-s=0$ 的两个根，且a, b分别为

$$a=\frac{u_0\beta-u_1}{\beta-\alpha},\ b=\frac{u_1-u_0\alpha}{\beta-\alpha},$$

令

$$x_m=a_1\alpha^m+a_2\beta^m,\ y_m=a_3\alpha^m+a_4\beta^m,$$

则对方程 $x_m=y_m$ 也有与定理15类似的结果。特别是对于用一般的代数数λ, μ去换x_m, y_m中的α,β,也有类似的结论。

§4 几个连续数问题

现在我们介绍几个与连续数有关的问题和结果。

Ⅰ. 丢番图方程$\sum\limits_{j=0}^{h}(x-j)^n=\sum\limits_{j=1}^{h}(x+j)^n$

Collignon[73] 曾经讨论了丢番图方程

$$\sum_{j=0}^{h}(x-j)^n=\sum_{j=1}^{h}(x+j)^n \tag{1}$$

的解，在$n=3$或4时，他证明了(1)无正整数解。

1963年，柯召[74]给出了方程（1）的完满解答。当$n=1$时，显然（1）给出正整数解

$$x=2\sum_{j=1}^{h}j=h(h+1);$$

当$n=2$时，易知（1）也仅有正整数解

$$x=4\sum_{j=1}^{h}j=2h(h+1)。$$

现设$n\geqslant 3$，由（1）得出

$$\begin{aligned}x^n&=\sum_{j=1}^{h}((x+j)^n-(x-j)^n)\\&=2\sum_{r=0}^{\left[\frac{n-1}{2}\right]}\binom{n}{2r+1}\sum_{j=1}^{h}j^{2r+1}x^{n-(2r+1)},\end{aligned}$$

即有

$$x=2\sum_{r=0}^{\left[\frac{n-1}{2}\right]}\binom{n}{2r+1}\sum_{j=1}^{h}j^{2r+1}x^{-2r}。$$

于是可以证明：

1） $3\leqslant n\leqslant 26$时方程（1）无正整数解。

2） 如果（1）有解，必有$h\equiv 0$或-1（mod8）。

3） 设$n\equiv 1$（mod 2），$n\geqslant 3$，$h=2^{3+s}l-1$ 或 $2^{3+s}l$，$s\geqslant 0$，$2\nmid l$，则$\sum_{j=1}^{h}j^n\equiv 2^{2s+4}\ (\mathrm{mod}\,2^{2s+5})$。

这里3)的证明用到如下的结果：

$$\sum_{j=1}^{h}j^n=\begin{cases}\dfrac{h^2(h+1)^2}{(n+1)!}f_n(h), & 当n\equiv 1(\mathrm{mod}2),\ n>1时；\\[2ex] \dfrac{h(h+1)(2h+1)}{(n+1)!}\varphi_n(h), & 当n\equiv 0(\mathrm{mod}2),\ n>0时。\end{cases}$$

这里$f_n(h)$和$\varphi_n(h)$都是h的整系数多项式。

利用1)～3)可得[73]

定理 1 方程（1）在$n\geqslant 3$时无正整数解。

Ⅱ．丢番图方程$y^m=x(x+1)\cdots(x+n-1)$

对于丢番图方程

$$y^m=x(x+1)\cdots(x+n-1),\ m>1,\ n>1, \quad (2)$$

从1933年开始，Obláth，Erdös，Rigge和Johnson 等先后对许多特殊情形作了研究[43]。1938 和 1939年，Rigge[75]和Erdös[76]各自独立地证明了

定理 2 方程

$$y^2=x(x+1)\cdots(x+n-1),\quad n>1 \quad (3)$$

仅有整数解 $y=0$ 。

这个定理的证明采用很特殊的方法。设 $y\neq 0$，$x+r=a_r x_r^2$（$r=0,\ 1,\ \cdots,\ n-1$），这里a_r均是无平方因子的整数，且仅有小于n的素因子。

首先证明a_r($r=0,\ 1,\ \cdots,\ n-1$）两两不同，为此先证$x\leqslant n$时(3)无解。这是因为在$x\leqslant n$时，必有一个素数p满足

$$x+n>p\geqslant\frac{x+n}{2}\geqslant x,$$

故$p\mid x(x+1)\cdots(x+n-1)$，但$p^2\nmid x(x+1)\cdots(x+n-1)$，这是不可能的。

于是$x>n$，由Sylvester和Schur的一个定理知，$x(x+1)\cdots(x+n-1)$必有一个素因子$q>n$。于是，对某$r\leqslant n-1$有$q^2\mid x+r$，故

$$x+r\geqslant(n+1)^2\Rightarrow x>n^2。$$

由此可证 a_r($r=0,\ 1,\ \cdots,\ n-1$）两两不同，因为不然设$a_r=a_s$，则

$$n > a_r x_r^2 - a_s x_s^2 = a_r(x_r^2 - x_s^2) > 2a_r x_r$$

$$\geqslant 2\sqrt{a_r x_r^2} = 2\sqrt{(x+r)} > \sqrt{x},$$

这与$x > n^2$矛盾。于是a_r（$r = 0, 1, \cdots, n-1$）两两不同，然后可证$n > 100$时，（3）无 $y \neq 0$ 的解。对 $n \leqslant 100$再单独处理一下。

利用柯召关于方程$x^2 - 1 = y^m$（$m > 1$）的结论，可以证明当$n = 3$和4时（2）仅有 $y = 0$的解。这是因为$n = 3$时(2)化为

$$x(x+1)(x+2) = y^m, \quad m > 1,$$

而（$x+1$，$x(x+2)$）$= 1$，故上式给出

$$x(x+2) = y_1^m,$$

由此整理得

$$(x+1)^2 - 1 = y_1^m, \quad m > 1。$$

在$n = 4$时，（2）化为

$$(x^2 + 3x + 1)^2 - 1 = y^m, \quad m > 1。$$

一般的情形，在1975年由 Erdös 和 Selfridge[77]得到了最后的解决，他们证明了

定理 3 方程（2）仅有 $y = 0$ 的整数解。

Ⅲ. 丢番图方程$\sum\limits_{j=0}^{h}(x+j)^n = (x+h+1)^n$

1900年，Escott[73] 提出了解丢番图方程

$$\sum_{j=0}^{h}(x+j)^n = (x+h+1)^n, \quad n > 1 \qquad (4)$$

的问题，他证明在$2 \leqslant n \leqslant 5$时，方程（4）除开$3^2 + 4^2 = 5^2$和$3^3 + 4^3 + 5^3 = 6^3$外，无其他正整数解 x，h 。

1962年，柯召和孙琦[78]证明了在$6 \leqslant n \leqslant 33$时，方程(4)无解，以及其他一些结果，如

1） 方程（4）的正整数解满足

$$1.1447n+0.6866<x+h<1.881n+0.468。$$

2） 在 $h\equiv 0 \pmod 4$ 时，方程（1）无正整数解。

3） 在$n\equiv 1 \pmod 2$ 时，方程（1）当$h\equiv 1 \pmod 4$ 时，或$h\equiv 2 \pmod 4$，$x\equiv 0 \pmod 2$ 时，均无正整数解。

1978年，柯召等[79]完全解决了 n 为奇数时，方程（4）的求解问题，得到了

定理 4 设$n>3$，$n\equiv 1 \pmod 2$，则方程（4）无正整数解。

对 $2|n$ 的情形还有

定理 5 设$2^{\beta}|n$，$\beta>0$，$h\not\equiv 1, 2 \pmod{2^{\beta+3}}$，则方程（4）无正整数解。

对于1)中的不等式，柯召和孙琦[80]还有一个详细的证明和更为精细的结果。

对于更为一般的方程

$$\sum_{j=0}^{n-1}(x+jr)^t=(x+nr)^t,\ t>2,\ n>1, \qquad (5)$$

Lebesgue[73]曾证明了在$t=3$时仅有正整数解$n=3$，$x=3r$。柯召和孙琦[81]在给出一系列引理的基础上，证明了在$4\leqslant t\leqslant 10$时，方程（5）无正整数解。

一个殊特的例子是方程

$$\sum_{j=1}^{m-1} j^n=m^n, \qquad (6)$$

Bowen猜想：方程（6)仅有正整数解$n=1$，$m=3$。1953年，Moser[82]证明了$m<10^{10^6}$时Bowen 猜想成立。1980年，阎发湘[83]证明了

定理 6 如果方程（6）有正整数解，则必有

$$m=\left[\frac{n-1}{\log 2}\right]+3\ 。$$

这些结果均是利用简单同余法，比较素数幂法和不等式法等初等方法证得的。例如定理 4 的证明如下：

可设$n>33$。由2）、3）知，只需考虑$h\equiv 2\pmod 4$，$x\equiv 1\pmod 2$和$h\equiv 3\pmod 4$两种情形。

a） $h\equiv 2\pmod 4$时，令$x+H=y$，$h=2H$，则方程（4）化为

$$(1+2H)y^n+2\binom{n}{2}\left(\sum_{j=1}^{H}j^2\right)y^{n-2}+\cdots+2\binom{n}{n-3}\left(\sum_{j=1}^{H}j^{n-3}\right)y^3$$

$$+2\binom{n}{n-1}\left(\sum_{j=1}^{H}j^{n-1}\right)y=(y+H+1)^n\ , \tag{7}$$

由于$x\equiv 1\pmod 2$，得出$y\equiv 0\pmod 2$和$y+H+1\equiv 0\pmod 2$。设$2^s\|y$，$s\geqslant 1$，对任意给定的奇数n，总存在α使得

$$2^{\alpha}<n<2^{\alpha+1}\ , \tag{8}$$

故 $\alpha<\frac{\log n}{\log 2}$，由1)知$y<2n$，即知 $2^s\leqslant\frac{\log y}{\log 2}<1+\frac{\log n}{\log 2}$，故得

$$s+\alpha+1<2+2\frac{\log n}{\log 2}<n。$$

现在（7）两端取模2^{s+3}得

$$\sum_{j=1}^{H}j^{n-1}\equiv 0\pmod 4。$$

设$\sum_{j=1}^{H}j^{n-1}\equiv 0\pmod{2^r}$，对$2\leqslant r\leqslant\alpha-1$ 中某一个r成立，则我们有[77]

$$\sum_{j=1}^{H}j^u\equiv 0\pmod{2^r},\quad r\leqslant u\leqslant n-3,\quad 2|u, \tag{9}$$

$$2^{r+s+1}\mid y^{n-u}\sum_{j=1}^{H}j^u,\quad 0\leqslant u<r,\quad 2|u。 \tag{10}$$

于是设 $\sum_{j=1}^{H} j^{n-1} \equiv 0 \pmod{2^r}$，对 $2 \leqslant r \leqslant \alpha-1$ 中某r成立，对（7）取模2^{s+r+2}得 $\sum_{j=1}^{H} j^{n-1} \equiv 0 \pmod{2^{r+1}}$。故对（7）继续取模 2^{r-s-2}，$r=2, \cdots, \alpha-1$ 得出

$$\sum_{j=1}^{H} j^{n-1} \equiv 0 \pmod{2^{\alpha}},$$

由此推出[77]

$$h \equiv -2 \pmod{2^{\alpha-2}},$$

注意到1)可知，上式给出

$$2^{\alpha-2} \leqslant h+2 \leqslant 2n,$$

这与（8）式矛盾。

b) $h \equiv 3 \pmod 4$ 时，与a)的证明完全类似，这里就不列出了。

§5 Fermat 大定理

大约在1637年，Fermat 声称他证明了如下的定理：

"丢番图方程

$$x^n + y^n = z^n, \quad n > 2 \tag{1}$$

没有正整数解"。

这就是著名的Fermat 大定理，但是直到今天人类也未能彻底证明这个定理。我们在第六章§4和第二章的§3中分别给出了$n=3,4$的证明(分别由Euler和Fermat 证明)。Kummer为了证明这个定理，创立了一门新的数论分支——理想数论。

由于$n>2$，故必有$4|n$或 $p|n$，p 为奇素数。于是证明Fermat大定理只要对$n=4$或$n=p$ 来证明就足够了。前者已经证明是对的，对后者方程（1）化为

$$x^p + y^p = z^p, \quad p>3\text{是素数。} \tag{2}$$

设$\theta=e^{2\pi i/p}$，$i=\sqrt{-1}$，是一个p次单位根，则（2）式可分解为

$$(x+y)(x+\theta y)\cdots(x+\theta^{p-1}y)=z^p。$$

现在我们来介绍Kummer 在域$Q(\theta)$中的工作[43]。

Ⅰ．因为θ满足不可化方程

$$x^{p-1}+\cdots+x+1=0,\quad x\in Q,$$

故$Q(\theta)$是$p-1$次域，称为$p-1$次分圆域。

Ⅱ．$Q(\theta)$中的整数为

$$\xi=a_0+a_1\theta+\cdots+a_{p-2}\theta^{p-2},\quad a_i\in Z。$$

显然$\xi^p\equiv a\pmod p$。

Ⅲ．$\pi=1-\theta$为$Q(\theta)$中的素数，且$p=\varepsilon\lambda^{p-1}$，$\varepsilon$为$Q(\theta)$的一个单位数，

Ⅳ．$Q(\theta)$中的仅有的单位根是$\pm\theta^r$，$r=0，1，\cdots，p-1$。$\varepsilon_r=\dfrac{\theta^r-1}{\theta-1}$是一个单位数且$\varepsilon_r$是整数，$N(\varepsilon_r)=1$。

Ⅴ．$Q(\theta)$中的任一个单位ε均可表为$\varepsilon=\theta^s\delta$，这里$0\leqslant s<p$，$\delta$是实单位数。

Ⅵ．设$Q(\theta)$的类数为h，则在$p\nmid h$时，p称为正规素数，而在$p|h$时，p称为非正规素数。

当p是正规素数和ε是$Q(\theta)$中的一个单位数满足$\varepsilon\equiv a\pmod{\pi^p}$，$a\in Z$时，必有，

$$\varepsilon=\varepsilon_0^p,$$

这里ε_0是$Q(\theta)$中的一个单位数。

利用这些工作，可以证明

定理 1 设p是正规素数，则方程（2）无$xyz\neq0$的整数解。

Kummer还给出判断p是否是正规素数的方法。

定理 2 设 $p>3$ 是素数，如果 p 不整除前 $\frac{p-3}{2}$ 个 Bernoulli数的分子，则p是正规素数。

有关Bernoulli数的定义及求法见第二章§7。

定理 3[73] 设$p\nmid xyz$，t表示x，y，z中任意两个的比，$\Phi_n(t)=t-2^{n-1}t^2+3^{n-1}t^3+\cdots+(-1)^{p-2}(p-1)^{n-1}t^{p-1}$，则方程（2）有解时可推出

$$\Phi_n(t)\ B_{\frac{p-n}{2}}\equiv 0\ (\bmod p),n=3,5,\cdots,p-2。\qquad (3)$$

由（3）式可推出

$$2^{p-1}\equiv 1\ (\bmod p^2)\ ,\qquad (4)$$

$$3^{p-1}\equiv 1\ (\bmod p^2)\ 。\qquad (5)$$

四十年代，Furtwängler用简单同余法重新证明了（4）和（5）（另一个结果见第三章§2）。人们已知，如果Fermat大定理第一情形成立，则对所有素数 $q\leqslant 43$均成立

$$q^{p-1}\equiv 1\ (\bmod p^2)。$$

Lehmer利用这个结果证明了$p\leqslant 25374887$时Fermat大定理第一情形成立。通过计算表明[84]，当 $p<31059000$时，仅有$p=1093$，$p=3571$ 满足（4），而当 $p<10752000$ 时 仅有$p=11$，$p=1006003$ 满足（5）。

最近，Granville[85] 利用一个幂数（定义见第五章§4）的猜想研究了同余式（4）。这个关于幂数的猜想是由Mollin和Walsh[86]提出来的，他们认为不存在三个连续幂数。如果这个猜想成立，则可以推出有无穷多个素数p 满足（4）。

1985年，Adleman 和 Heath—Brown[87] 证明了有无穷多个素数p使Fermat大定理第一情形成立。即有

定理 4 设$s=\{p:p$使Fermat 大定理第一情形成立$\}$，则 $\#\{p\in s:p\leqslant x\}>>x^{0.687}$。

与Fermat大定理第一情形紧密相连的Kummer—Mirimanoff同余式和 Eisenstein 同余式也一直吸引着人们的兴趣，有许多关于Fermat 大定理的工作都是基于这两个同余式的。

所谓Kummer—Mirimanoff 同余式是指：设p 是奇素数，存在互素的整数a，b，c满足$a^p+b^p+c^p=0$且$p\nmid abc$，则有同余式

$$b_n\sum_{k=1}^{p-1}\frac{u^n}{k^n}\equiv 0\ (\bmod p)\quad (n=0,\ 1,\ \cdots,\ p-2)\qquad (6)$$

成立，这里b_n由$\frac{t}{e^t-1}=\sum_{m=0}^{\infty}b_m\frac{t^m}{m!}$定义，且 $u=\frac{-a}{b}$ 。注意，b_m与Bernoulli 数B_m间有如下的关系（见第五章§7；有时b_m也称为 Bernoulli 数）：

对所有$n\geqslant 1$，$b_{2n-1}=0$和$b_{2n}=(-1)^{n+1}B_n$。

于是（6）式可化为

$$B_n\sum_{k=1}^{p-1}\frac{u^{2n}}{k^{2n}}\equiv 0\ (\bmod p)\quad \left(n=0,\ 1,\ \cdots,\ \frac{p-3}{2}\right)。$$

1985年，Thaine[88]重新给出了Kummer—Mirimanoff 同余式的证明，同时还证明了

定理 5 对所有n，$1\leqslant n\leqslant\frac{p-3}{2}$，如果$B_n\equiv 0(\bmod p)$，则有

$$\sum_{k=1}^{p-1}k^{2n-1}u^k\equiv 0\ (\bmod p)。$$

Jothilingan[89]给出了 Eisenstein 同余式

$$2^{p-1}\equiv 1+p\left(1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{p-2}\right)(\bmod p^2)$$

的一个推广。

利用人们对 Fermat 大定理的一些工作，Wagstaff 于1978年在大型计算机的帮助下证明了$p<125000$时Fermat大定理成立。而Heath—Brown[10]证明了对“几乎所有”的n，方程（1）无正整数解。即有

定理 6 设$H(N)$表$n\leqslant N$且使（1）有解的n的个数，则有$\lim\limits_{N\to\infty}\frac{H(N)}{N}=0$。

这一定理的证明主要是基于Faltings[9]1983年的一个著名结果，即（参阅第三章§5）

定理 7 设$n\geqslant 4$，则方程（1）最多只有有限组满足$(x,y)=1$的解。

推论 1 设$n=p^r$，p为奇素数，r为充分大的正整数，则方程（1）无解。

这一段时间，似乎是解决 Fermat 大定理的时期，一个又一个的重要突破接踵而来。最近，人们把Fermat 方程与椭圆曲线方程 $y^2=x^3+ax^2+bx+c$（a，b，c 是常数）联系起来，得到了 Fermat 大定理不成立的一些椭圆曲线。由人们对椭圆曲线的认识使我们看到了证明Fermat 大定理的希望。

另一方面，利用简单同余法和其他一些初等方法的技巧，对Fermat大定理的第一情形以及Fermat 大定理的相关方程也有过一些重要工作，这方面的文献多得无法计数。我们这里只能举一些例子。

定理 8 设$q=2hp+1$是素数，如果 $q\nmid D_{2h}$且$p^{2h}\not\equiv 1\pmod{q}$，则方程（2）无$p\nmid xyz$ 的整数解。
这里

$$D_{2h}=\begin{vmatrix} \binom{2h}{1} & \binom{2h}{2} \cdots & \binom{2h}{2h-1} & 1 \\ \binom{2h}{2} & \binom{2h}{3} \cdots & 1 & \binom{2h}{1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \binom{2h}{1} \cdots & \binom{2h}{2h-2} & \binom{2h}{2h-1} \end{vmatrix}。$$

推论 2 设p是一个奇素数，则当$2p+1$或$4p+1$也是素数时，方程（2）无$p\nmid xyz$的整数解。

1974年，Perisastri[92] 曾用一个十分简单的方法给出了推论2的一个证明。同时利用（4）式他还证明了

定理 9 设$p=2^n-1$是Mersenne 素数，则方程（2）没有$p\nmid xyz$的解。

定理10 设$p=2^{2^n}+1$是 Fermat 素数，则方程（2）没有$p\nmid xyz$的解。

这两个定理的证明，需要用到x^t（$t>1$）可表为

$$x^t=(x-a)^2g(x)+ta^{t-1}x+a^t(1-t) \qquad (7)$$

的结论，这里$g(x)$是整系数多项式，a是任意整数。因为

$$x^t=(x-a)^2g(x)+ax+b \qquad (8)$$

是众所周知的，这里a，b是待定整数。故对（8）两端求导得出

$$tx^{t-1}=(x-a)[(x-a)g'(x)+2g(x)]+a。 \qquad (9)$$

令$x=a$，则由（9）得出$a=ta^{t-1}$，再由（8）得出$b=a^t(1-t)$，于是（7）成立。

利用（7）式极易证明定理9和定理10。例如在$p=2^n-1$时，由Mersenne素数的性质知$n\mid p-1$，令$p-1=nt_1$，$t_1>1$。于是在（7）中取$t=t_1$，$a=1$，$x=2^n$得

$$2^{p-1}=p^2g(2^n)+t_1p+1,$$

由此推出$2^{p-1} \not\equiv 1 \pmod{p^2}$。而在$p = 2^{2^n}+1$时，令$t = \frac{p-1}{2^n}$，

$a = -1$，$x = 2^{2^n}$代入（7）得（注意 $2|t$）

$$2^{p-1} = p^2 g(2^{2^n}) - \frac{p-1}{2^n} p + 1,$$

这仍给出$2^{p-1} \not\equiv 1 \pmod{p^2}$。这就证明了定理9和10。

对于与 Fermat 方程相关的方程

$$x^p - y^p = Dz^2,\ D>0,\ p>3\text{是素数},\ (x,y)=1,\quad (10)$$

当D是一个平方数(或等价地设$D=1$)时，孙琦和曹珍富[93]证明了

在$y \equiv 2 \pmod 4$或$y \equiv 4 \pmod 8$时，（10）均无整数解。同时还证明了偶指数的 Fermat 方程

$$x^{2p} + y^{2p} = z^{2p},\quad (x, y)=1,\ p>3\text{ 是素数}$$

有解时，可推出$8p|x$或$8p|y$。这是对Terjanian[94]在1977年证明的$2p|x$或$2p|y$ 的一个改进。曹珍富[39]对D不是平方数时，证明了如下的

定理11 设D无平方因子，且不被 $2mp+1$ 形的素数整除，则在$2|z$，$p\nmid z$时，或$2\nmid z$，$p|z$时，方程(10)无整数解。

由此可推出[95]，设D的条件同定理11，则在$y\equiv 2 \pmod 4$或$y\equiv 4 \pmod 8$时，方程（10）无整数解。

对于比偶指数的 Fermat 方程更为一般的方程

$$x^{2p} + y^{2p} = z^2,\quad (x, y)=1,\ p>3\text{是素数},\quad (11)$$

$$x^{2p} - y^{2p} = z^2,\quad (x, y)=1,\ p>3\text{是素数},\quad (12)$$

$$x^{2p} + y^{2p} = z^p,\quad (x, y)=1,\ p>3\text{是素数},\quad (13)$$

$$x^{2p} - y^{2p} = z^p,\quad (x, y)=1,\ p>3\text{是素数},\quad (14)$$

曹珍富（部分结果见[96]）证明了（11）和（13）有解时可推出$4p|x$ 或 $4p|y$；（12）有解时可推出$8p|y$ 或 $4p|z$；而

(14) 有解时可推出$4p|x$或$4p|y$或$8p|z$。以上结果的证明都可使用二次剩余法得到（见第二章§5）。

参考文献

[1] 曹珍富，科学通报，6 (1985)，475。

[2] Nagell, T., Norsk Mat. Forenings Skrifter, Serie I, No.13 (1921).

[3] 曹珍富, Proc. Amer. Math. Soc., 98 (1986), 11—16; 数学季刊,1(1987), 91—97。

[4] 曹珍富，数学汇刊，1 (1984)，51—56。

[5] 曹珍富，河池师专学报，1 (1987)，1—8。

[6] Tartakowski, V.A., Izvestia Akad. Nauk SSSR, 20 (1926), 301—324.

[7] Ljunggren, W., C.R.Dixième Congrès Math. Scandinaves 1946, 265—270.

[8] Siegel, C.L., Math. Ann., 114 (1937), 56—68.

[9] 曹珍富，自然杂志，2 (1987)，151。

[10] 曹珍富，哈尔滨工业大学学报，2 (1987)，122—124。

[11] 王笃正，曹珍富，扬州师院学报(自然科学版)，2 (1985)，16—18。

[12] Landau, E. and Ostrowski, A., Proc. London Math.Soc.,(2), 19(1920),276—280.

[13] Thue, A., Arch. Math. Naturv. Kristiania, Nr. 16, 34 (1917).

[14] Ljunggren, W., Norske Vid. Selsk. Forh.,

Trondhjem 15, No. 30 (1942), 115—118。
[15] Ljunggren, W., Norske Vid. Selsk. Forh., Trondhjem 17, No. 23 (1944), 93—96。
[16] Ljunggren, W., Norske Vid. Selsk. Forh., Trondhjem 16, No. 8(1943), 27—30.
[17] Kawamoto, M., Mem. Gifu Nat. Coll. Tech., 20 (1985), 55—56.
[18] Ljunggren, W., Arkiv för Mat., Astronomi och Fysik, v. 29A, No. 13, Stockholm (1943), 1—11.
[19] Nagell, T., Archiv der Math., Bd 5, S. 53, Zürich 1954。
[20] Nagell, T., Arkiv för Mat., 3 (1955), 103—112.
[21] Brown, E., J. Reine Angew. Math., 291 (1977), 118—127.
[22] Toyoizumi, Acta Arith., 42(1983), 303—309。
[23] 曹珍富，科学通报，7 (1986), 555—556。
[24] Lebesgue, V.A., Nouv. Ann., Math., (1)9 (1850), 178—181.
[25] Störmer, C., L'intermédiaire des Math., 3 (1896), 171.
[26] Brown, E., J. Reine Angew. Math., 274/275 (1975), 385—389.
[27] Nagell, T., Norsk Mat. Forh. Skrifter, Ser. I, Nr. 13, Kristiania 1923.
[28] Ljunggren, W., Pacific J. Math., 14(1964),

585—596.

[29] Ljunggren, W.,Norske Vid. Selsk. Forh., Trondhjem 18, No. 32 (1945), 125—128.

[30] Ljunggren, W.,ibid, Trondhjem 29, No. 1 (1956), 1—4.

[31] Nagell, T., Norsk Mat. Forenings Skrifter, Serie I, No. 2 (1921), 14pp.

[32] Ljunggren, W., Acta Math., 75 (1942), 1—21.

[33] Persson, B., Ark. Mat., 1(1949), 45—57.

[34] Stolt, B., Arch. Math., 8(1957),393—400.

[35] Ljunggren, W., Monatsh. Math.,75(1971), 136—143.

[36] Ljunggren, W., Acta Arith.,21 (1972), 183—191.

[37] Skolem, Th.,8de Skand. Mat. Kongress, Stockholm 1934, 163—188.

[38] 曹珍富，西南师范学院学报（自然科学版），2 (1985)，69—73。

[39] 曹珍富，东北数学，2 (1986)，219—227。

[40] 曹珍富，数学研究与评论，3 (1987)，414。

[41] 孙琦，四川大学学报（自然科学版），1(1987)，19—23。

[42] 柯召，四川大学学报（自然科学版），4(1959)，15—18。

[43] Mordell, L. J., Diophantine equations, Academic Press, London and New York,

1969.

[44] 柯召，四川大学学报（自然科学版），1(1962)，1—6；Sci. Sin., 14 (1965), 457—460。

[45] Chein, E.Z., Proc. Amer. Math. Soc., 56 (1976), 83—84.

[46] Rotkiewicz, A., Acta Arith., 42 (1983), 163—187.

[47] 曹珍富，西南师范大学学报（自然科学版），2 (1987), 16—19。

[48] Cassels, J.W.S., Proc. Comb.Phil.Soc., 56 (1960), 97—103.

[49] 柯召，四川大学学报（自然科学版），2(1962)，1—6。

[50] Tijdeman, R., Acta Arith., 29 (1976), 197—209.

[51] Siegel, C.L., Math. Ann., 144 (1937), 57—68. Also Gesammelte Abhandlungen, Ⅱ (1966).

[52] Domar, Y., Math. Scand., 2(1954),29—32.

[53] af Ekenstam, A., Dissertation (1959). Uppsala, Almqvist and Wiksells.

[54] Hyyrö, S., Ann. Acad. Sci. Fennicae, Series A. I., 355 (1964), 1—50.

[55] Skolem, T., Chr. Michelsens Inst. Beretn., 4 (1934), Nr. 6, Bergen.

[56] Ljunggren, W., Oslo Vid—Akad Skrifter, 1 (1936), No. 12.

[57] Ljunggren, W., Arch. Math. Naturv., 48 (1946), Nr.7, 26—29.
[58] 曹珍富，哈尔滨工业大学学报，4 (1987)，113—121。
[59] Baker, A., Q.J.Math., Oxf. II. Ser. 15 (1964), 375—383.
[60] Evertse, J.-H., Math. Centrum. Amsterdam, (1983), 1—127.
[61] Bombieri, E.and Schmidt, W.M., Invent. Math., 88 (1967), 69—81.
[62] Nagell, T., Norsk Mat. Tidsskr, 1920, 75—78.
[63] Ljunggren, W., Norsk Mat. Tidsskr, 25 (1943), 17—20.
[64] 柯召，四川大学学报（自然科学版），2(1960)，57—64。
[65] Guy, R.K., Unsolved problems in number theory, Springer, New York, 1981.
[67] Inkeri,K.,Acta Arith.,21(1972),299—311.
[68] Shorey, T. N., Indagationes Math., 48 (1986), 345—351.
[69] Shorey, T.N., Math. Proc. Camb. Philos. Soc., 99 (1986), 195—207.
[70] Shorey, T. N., Indagationes Math., 48 (1986), 353—358.
[71] Shorey, T.N., Acta Arith., 41 (1982), 255—260.

[72] Shorey, T.N., Acta Arith., 43 (1984), 317—331.
[73] Dickson, L.E., History of the Theory of Numbers, Vol. Ⅱ, 1952, 564.
[74] 柯召，四川大学学报（自然科学版），1(1963)，1—9。
[75] Rigge, O., IX. Skan. Math. Kongr. Helsingfors (1938).
[76] Erdös, P., J. London Math. Soc., 14 (1939), 194—198.
[77] 柯召，孙琦，谈谈不定方程，上海教育出版社 (1980)，P. 123。
[78] 柯召，孙琦，四川大学学报（自然科学版），2 (1962)，9—18。
[79] 柯召，孙琦，四川大学学报（自然科学版），2—3 (1978)，19—24。
[80] 柯召，孙琦，四川大学学报（自然科学版），4 (1982)，1—3。
[81] 柯召，孙琦，四川大学学报（自然科学版），2 (1963)，33—42。
[82] Moser, L., Scripta Math., 19 (1953), 84—88.
[83] 阎发湘，辽宁大学学报(自然科学版),1(1980)，1—10。
[84] Kloss, K.E., J. Res. Nat. Bur. Standards Sect. B, 693 (1965), 335—336.
[85] Granville, A., C.R. Math. Acad. Sci.,

Soc. R. Can., 8 (1986), 215—218.
[86] Mollin, R.A. and Walsh, P.G., C.R. Math. Acad. Sci., Soc. R. Can., 8 (1986), 109—114.
[87] Adleman, L.M. and Heath—Brown, D.R., Invent. Math., 79 (1985), No.2, 409—416.
[88] Thaine, F., J. Number Theory, 20(1985), No.2, 128—142.
[89] Jothilingan, P., Acta Math. Hung., 46 (1985), 265—267.
[90] Heath—Brown, D.R., Bull. London Math. Soc., 17 (1985), No.1, 15—16.
[91] Faltings, G., Invent. Math., 73 (1983), No.3, 349—366.
[92] Perisastri, M., J. Reine Angew. Math., 265 (1974), 142—144.
[93] 孙琦，曹珍富，数学年刊，7A (1986), No.5, 514—518。
[94] Terjanian, G., C.R. Acad. Sci. Paris, 285 (1977), 973—975.
[95] 曹珍富，哈尔滨电工学院学报，2 (1988), 184—189。
[96] 曹珍富，自然杂志，5 (1987), 393—394。

第九章　指数丢番图方程

近年来，一方面指数丢番图方程本身有许多新的进展；另一方面，在群论，组合论和编码理论中又提出了若干指数丢番图方程来，这方面有许多重要工作。本章我们将较详细地介绍有关指数丢番图方程研究的成果和方法。

§1　两个乘幂之差

把一个数表为两个乘幂之差的问题引人注目。特别是把2表为两个素数乘幂之差，在组合论的差集中有重要应用。1958年，Stanton和Sprott[1]建立了参数为 $v=p^mq^n$，$k=\frac{v-1}{2}$，$\lambda=\frac{v-3}{4}$的阿贝尔群差集，其中p，q，m，n满足如下关系

$$p^m-q^n=2,\ p,\ q\text{是素数},\ m>1,\ n>1. \qquad (1)$$

1967年，Hall[2]问：除开$p=3$，$m=3$，$q=5$，$n=2$外，方程(1)是否存在另外的解？1984年，孙琦和周小明[3]证明了

定理 1　设$p=q+2$，-2模 p 的次数 l满足$3\mid l$，且$f=q^2+q+1$是一个素数，满足$p^{q+1}\not\equiv 1(\bmod f)$，则方程(1)无解。

1985年，利用Pell方程的解法（参阅第二章§6），曹珍富[4][5]彻底解决了方程(1)当$p=q+2$的情形，即有

定理 2　设$p=q+2$　则方程(1)无解。

在$\max(p, q)<100$时，曹珍富[6]还给出了方程(1)的全部解，这个工作支持我们猜想：除开 $p=3$，$m=3$，$q=5$，$n=2$外，方程(1)不存在别的解。

由于方程$x^2+2=y^n(n>1)$仅有正整数解$x=5$，$y=3$，$n=3$（见第八章§2），故方程(1)在$2\mid n$时仅有解$3^3-5^2=2$。下设$2\nmid n$。

定理 3[7] 方程(1)有$2\nmid n$的解的充要条件是方程

$$x^2+2qy^2=p^z,\ (x,y)=1,\ z>0 \tag{2}$$

有解，而且如果x_1，y_1，z_1为其最小解（即方程(2)的所有解中满足$x>0$，$y>0$使z为最小的那组解），则有

$$x_1=q^n-1,\ y_1=2q^{\frac{n-1}{2}},\ z_1=2m。$$

由于方程(2)的最小解的唯一性，可知有如下的

推论 1 对给定的p，q，方程(1)最多有一组解。

推论 2 设 $p=qa^2+2b^2$，$a,b\in Z$，则方程(1)无解。

证 由于

$$(qa^2-2b^2)^2+2q(2ab)^2=(qa^2+2b^2)^2,$$

故知$z_1\leqslant 2$。由定理3知$2m=z_1\leqslant 2$，即$m\leqslant 1$ 与方程(1)中$m>1$矛盾。证毕。

对于更为一般的方程，Hugh Edgar[8]提出了如下问题：方程

$$p^m-q^n=2^h \text{（对给定的素数}p,q\text{和整数}h\text{）的解}(m,n) \tag{3}$$

有多少？是否最多只有一个？仅有有限个吗？曹珍富和王笃正[9]解决了这个问题，证明了

定理 4 方程(3)满足$m>1$，$n>0$的解(m,n)最多只有一个。

我们是通过对三个变元的指数丢番图方程

$$p^x-q^y=2^z,\ p,\ q\text{是奇素数} \tag{4}$$

的研究来实现的。由于$2|y$时方程(4)化为

$$(q^{\frac{y}{2}})^2+2^z=p^x$$

的形状，故由第八章§2关于方程 $x^2+2^m=y^n\ (n>1)$ 的结果知，在$x>1$，$2|y$时方程(4)仅有解[10]

$3^3-5^2=2$，$3^4-7^2=2^5$，$5^2-3^2=2^4$，$5^3-11^2=2^2$。

以下设$2\nmid y$。

定理 5 如果方程(4)存在$2\nmid y$，$2|z$的解，则方程$X^2+qY^2=p^Z$必有整数解，且设Z_1是任给正整数X_1，Y_1使得$X_1^2+qY_1^2=p^{Z_1}$的最小者，则必有

$$X_1=2^{\frac{z}{2}},\ Y_1=q^{\frac{y-1}{2}},\ Z_1=x。$$

定理 6 如果方程(4)存在$2\nmid y$，$2\nmid z$的解，则方程$X^2+2qY^2=p^Z$必有正整数解，且设Z_0是对于任给正整数X_0，Y_0使得$X_0^2+2qY_0^2=p^{Z_0}$的最小者，则必有

$$X_0=|q^y-2^z|,\quad Y_0=2^{\frac{z+1}{2}}q^{\frac{y-1}{2}},\ Z_0=2x$$

定理 5，6的证明，都要用到第三章§1的例5。如果方程(4)有$2\nmid y$，$2|z$的解，则(4)可整理成

$$\left(2^{\frac{z}{2}}\right)^2+q\left(q^{\frac{y-1}{2}}\right)^2=p^x,$$

故得

$$2^{\frac{z}{2}}+q^{\frac{y-1}{2}}\sqrt{-q}=\pm(X_1+Y_1\sqrt{-q})^t\text{或}\pm(X_1-Y_1\sqrt{-q})^t,\qquad x=tZ_1。\tag{5}$$

如果方程(4)有$2\nmid y$，$2\nmid z$的解，则由(4)整理得

$$\left(q^y-2^z\right)^2+2q\left(2^{\frac{z+1}{2}}q^{\frac{y-1}{2}}\right)^2=p^{2x},$$

由此得出

$$|q^y-2^z|+2^{\frac{z+1}{2}}q^{\frac{y-1}{2}}\sqrt{-2q}=\pm(X_0+Y_0\sqrt{-2q})^t$$

或 $\pm(X_0-Y_0\sqrt{-2q})^t$， $2x=tz_0$。 (6)

然后证明(5)，(6)中的$t=1$即得定理5、6。而由定理5、6及方程$x^2+2^m=y^n$的结果容易推出定理4。由定理5、6还可以证明[11]

定理 7 方程(4)在$2\nmid y$时最多只有一组正整数解。

故由方程$x^2+2^m=y^n(n>1)$的结果可推出比Hugh Edgar问题要求的结论更强的

推论 设$\max(p,q)>7$，则方程(4)适合$x>1$的正整数解至多只有一个。

在解决Hugh Edgar 问题之前，曹珍富[12]对方程(4)还证明了

Ⅰ. 设$p=qt^2+4$，$q\not\equiv1(\mathrm{mod}\,8)$，则方程(4)除开$t=q^k$ $(k\geqslant0)$时仅有解$(x,y,z)=(1,2k+1,2)$外，无其他的非负整数解。

Ⅱ. 设$q=pt^2-4$，$p\not\equiv1(\mathrm{mod}\,8)$，则方程(4)除开

1) $p\neq3$，$t=p^k$，$k\geqslant0$仅有解$(x,y,z)=(2k+1,1,2)$和

2) $p=3$，仅有解(1，0，1)，(2，0，3)，且当$t=3^k$ $(k>0)$时还有解$(2k+1,1,2)$外，无其他的非负整数解。

Ⅲ. 设$p=q^{2k+1}+2$，$k\geqslant0$且$q\not\equiv1(\mathrm{mod}\,8)$，则方程(4)除开$(1,2k+1,1)$外，无其他非负整数解。

这些结果在解指数丢番图方程$a^x+b^y=c^z$（见§2）时都有重要应用。对于丢番图方程

$$a^x-b^y=(2p)^z,\quad p\text{是奇素数} \tag{7}$$

（这里a，b不一定是素数），Perisastri[13]讨论了$p=5$的情形，此时方程(7)化为

$$a^x-b^y=10^z。\tag{8}$$

定理 8 设$(a,\ b)\equiv(13,\ 3)\ (\bmod 20)$，则方程(8)无$z\neq1$的非负整数解。

曹珍富[14]证明了

定理 9 设$a\equiv3,7(\bmod 10),b\equiv11,19,21,29(\bmod 40)$，则方程(8)无$z\neq2$的非负整数解。

1982年，Toyoizumi[15]对方程(7)证明了在$p\equiv a\equiv 5(\bmod 8)$，$b\equiv3(\bmod 8)$且$p\nmid ab$时，方程(7)无$z\geqslant3$的非负整数解。

这个结论是不对的，例如我们有

$$(4p^4+1)^2-(4p^4-1)^2=(2p)^4。$$

曹珍富[16][17]在1985在对更一般的方程

$$a^x-b^y=(2p^s)^z,\tag{9}$$

这里s为非负整数，p为奇素数，且$p\nmid ab$，证明了

定理10 设$(a,\ b)\equiv(5,\ 3)(\bmod 8)$，则方程(9)除开$a=4p^{4s}+1$，$b=4p^{4s}-1$时有解$x=y=2$，$z=4$外，无$z\geqslant3$的非负整数解。

在$(a,\ b)\equiv(5,\ 3)(\bmod 8)$及$z\geqslant3$时，对(9)取模8知$2|x$，$2|y$，故用分解因子法可以证明定理10。与定理10类似地，我们还有

定理11 设$(a,\ b)\equiv(3,5),(\pm3,7),(7,\pm3)(\bmod 8)$，则方程(9)除开$3^4-7^2=2^5$外，无$z\geqslant4$的非负整数解。

最近，曹珍富和王笃正[18]对方程(7)在$\left(\frac{a}{p}\right)=-1$，

$\left(\frac{b}{p}\right)=1$ 或 $\left(\frac{a}{p}\right)=1$，$\left(\frac{b}{p}\right)=-1$ 或 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)=-1$ 时，得出了方程(7)无解的一系列结果。

§2 丢番图方程 $a^x+b^y=c^z$

给定正整数 a，b，c，求方程

$$a^x+b^y=c^z \tag{1}$$

的解是丢番图方程中一个重要的课题，其中尤为引人注目的是 a，b，c 均是素数以及 a，b，c 取商高数组的情形。

Ⅰ．a，b，c 均是素数。这时方程(1)化为

$$a^x+b^y=c^z,\quad a,b,c\text{是不同的素数。} \tag{2}$$

1958年，Nagell[19]首先求出了 $\max(a,b,c)\leqslant 7$ 时方程(2)的全部非负整数解，得到了下表：

序	方程	全部非负整数解 (x,y,z)
1)	$5^x=3^y+2^z$	(1,1,1),(1,0,2),(2,2,4)
2)	$3^x=5^y+2^z$	(1,0,1),(3,2,1),(2,1,2),(2,0,3)
3)	$2^x=5^y+3^z$	(1,0,0),(2,0,1),(3,1,1),(5,1,3),(7,3,1)
4)	$7^x=3^y+2^z$	(1,1,2)
5)	$3^x=7^y+2^z$	(1,0,1),(2,1,1),(2,0,3),(4,2,5)
6)	$2^x=7^y+3^z$	(1,0,0),(2,0,1),(3,1,0),(4,1,2)
7)	$7^x=5^y+2^z$	(1,1,1)
8)	$5^x=7^y+2^z$	(1,0,2)
9)	$2^x=7^y+5^z$	(1,0,0),(3,1,0),(5,1,2)

Nagell 对方程3)和9)的证明用了很长的篇幅且用了很深的代数数论和 p—adic 方法（参阅第三章）。

1959年，Makowski[20]求出了方程

$$2^x+11^y=5^z$$

的全部非负整数解，即$(x,y,z)=(2,0,1)(2,2,3)$。

1976年，Hadano[21]考虑了$11\leqslant \max(a, b,c)\leqslant 17$ 的情形，给出了此时除方程

$$3^x+13^y=2^z \tag{3}$$

外的全部非负整数解。Uchiyama[22]解决了方程(3)，他证明了方程(3)的全部非负整数解是(0,0,1),(1,0,2),(1,1,4)。

1984年，孙琦和周小明[3]给出了$\max(a,b,c)=19$ 时方程(2)的全部非负整数解。

1985年，杨晓卓[23]又给出了$\max(a,b,c)=23$时方程(2)的全部解。

这些关于方程(2)的工作，都是把方程(2)化成若干具体的指数丢番图方程，然后采用一个一个分别求解的方法，使$\max(a,b,c)$不断放大。我们看到，使用这种方法，每把$\max(a,b,c)$推进一步都十分困难。

1986年，曹珍富[24] 把方程(2)化为如下的两个丢番图方程

$$a^x+b^y=2^z，a，b\text{是不同的奇素数，} \tag{4}$$

$$a^x-b^y=2^z，a，b\text{是不同的奇素数。} \tag{5}$$

然后，对方程(4)，(5)进行一些定性研究，可以把$\max(a, b, c)$放大到100，并且使用我们的方法可以把$\max(a,b,c)$继续放大。

对于方程(4)，我们有

定理 1 设 $29\leqslant\max(a, b)\leqslant 97$，则方程(4)除开下面11种情形外，均无正整数解：

$3^4+47=2^7$，$7^2+79=2^7$，$17+47=2^6$，$41+23=2^6$，$97+31=2^7$，$3^3+37=2^6$，$3+61=2^6$，$11+53=2^6$，$59+5=2^6$，$3+29=2^5$，$67+61=2^7$。

对于方程(5)，我们在§1中已经证明了很一般的定理(见§1的定理7 及推论)。利用§1中的结果，加上简单同余法，就可以给出 $\max(a,b)<100$ 时方程(5)的全部正整数解，此时共有49对 (a,b) 使(5)有正整数解*。

由于在 $29\leqslant\max(c,b)\leqslant 97$ 时，方程(4)可化为248个具体的指数丢番图方程，方程(5)化为 2×248 个具体的指数丢番图方程，因此用一个一个分别求解的方法难以把 $\max(a,b,c)$ 推进到100。

我们猜想：当 $\max(a,b,c)>7$ 时，方程(2)最多只有一组正整数解 (x,y,z)。这在 $\max(a,b,c)<100$ 时已经成立。

Ⅱ。a,b,c 取商高数组。我们知道，商高数组 a,b,c 满足

$$a^2+b^2=c^2,$$

故此时方程(1)有正整数解 $x=y=z=2$。1956年，Jeśmanowicz[25]猜测：当 a,b,c 取商高数组时，丢番图方程(1)仅有正整数解 $x=y=z=2$。这一猜测至今只证明了对一些较为简单的商高数组是正确的，例如对于

$$a=2n+1,\quad b=2n(n+1),\quad c=2n(n+1)+1, \tag{6}$$

Sierpiński[26] 证明了 $n=1$ 时以及 Jeśmanowicz[25]证明了 $n=2,3,4,5$ 时，猜想是正确的。他们都只用了简单同余法。实际上结合分解因子法可使证明大大简化。例如在 $n=1$ 时方程(1)化为

$$3^x+4^y=5^z,\quad x>0,\quad y>0,\quad z>0。 \tag{7}$$

对(7)取模3得出 $2\mid z$，设 $z=2z_1$，则(7)化为

$$(5^{z_1}-2^y)(5^{z_1}+2^y)=3^x,$$

由此得出

$$5^{z_1}-2^y=1,\quad 5^{z_1}+2^y=3^x,$$

---

* 见曹珍富，科学通报，Vol.33(1988)，No.3，237.

这就给出$z_1=1$，$y=2$，$x=2$，即(7)仅有$x=y=z=2$的正整数解。

1958年，柯召[27][28]用简单同余法和分解因子法对(6)中的商高数组证明了

定理 2 在$n\equiv 1,3,4,5,7,9,10,11 \pmod{12}$时，Jeśmanowicz猜想都成立。如果存在素数$p\equiv 3 \pmod 4$或$p\equiv 5 \pmod 8$使得$2n+1\equiv 0 \pmod p$，则对(6)中的商高数组Jeśmanowicz猜想也成立。

定理 3 在$n\equiv 2 \pmod 5$，$n\equiv 3 \pmod 7$，$n\equiv 4 \pmod 9$，$n\equiv 5 \pmod{11}$，$n\equiv 6 \pmod{13}$或$n\equiv 7 \pmod{15}$时，Jeśmanowicz猜想成立。

由此可推出$n<96$时猜想成立。

1960年，饶德铭[29]利用柯召的方法进一步证明了：对(6)中的数，当$n\equiv 2,6 \pmod{12}$时，Jeśmanowicz猜测成立。由此可知，对(6)中的数还剩下$n\equiv 0,8 \pmod{12}$没有解决。

1964年，柯召和孙琦[30]讨论了$n\equiv 0,8 \pmod{12}$的情形，并证明了在$n<1000$时Jeśmanowicz猜测成立。稍后，柯召[31]又把1000改进为6144。

1965年，Dem'janenko[32]彻底地解决了(6)中的数即他证明了

定理 3 对(6)中的商高数组，Jeśmanowicz猜测成立。

对于商高数组

$$a=m^2-1,\ b=2m,\ c=m^2+1,\ m>1, \tag{8}$$

1959年，陆文端[33]首先解决了$m=2^n$的情形，即他证明了

定理 4 丢番图方程

$$(4n^2-1)^x+(4n)^y=(4n^2+1)^z$$

仅有正整数解$x=y=z=2$。

1961年，Józefiak[34] 证明了定理 4 中的一个极特殊的情形，即他解决了(8)中数当$m=2^r p^s$，r,s是正整数，p是素数时的情形。

1965年，Dem'janenko[32]对 (8)中任意m证明了 Jeśmanowicz猜想成立。

我们在第二章的§2中曾给出商高数组的通解，在$(a,b,c)=1$ 时通解是

$$a=s^2-t^2,\ b=2st,\ c=s^2+t^2 \tag{9}$$

这里$s>t>0$，$(s,t)=1$, $s+t\equiv1(\bmod 2)$。柯召[35]在1959年首先对(9)中的商高数组进行了研究，他证明如下两个定理。

定理 5 设$s=2n$和t均不含有$4k+1$形素因子，且

1) $n\equiv2(\bmod 4)$，$t\equiv3(\bmod 8)$，或

2) $n\equiv2(\bmod 4)$，$t\equiv5(\bmod 8)$，$2n+t$ 含有$4k-1$形素因子，或

3) $n\equiv0\ (\bmod 4)$, $t\equiv3,5(\bmod 8)$，

则 Jeśmanowicz 猜测成立。

定理 6 设$s=3n$，$t=2m$均不含有$4k+1$ 形素因子，且$\sqrt{2}(2m)>3n>2m>0$ 或 $3n>8m>0$。则在

1) $m\equiv2(\bmod 4)$，$n\equiv1(\bmod 8)$时，或

2) $m\equiv2(\bmod 4)$，$n\equiv7(\bmod 8)$，$3n+2m$含有$4k-1$形素因子时，或

3) $m\equiv0(\bmod 4)$，$n\equiv1,7(\bmod 8)$时，Jeśmanowicz猜测成立。

这两个定理的证明思路是：在所设条件下可证 $2|x$，$2|z$，设$x=2x_1$，$z=2z_1$，则(1)式化为

$$(s^2-t^2)^{2x_1}+(2st)^y=(s^2+t^2)^{2z_1},$$

即有

$$(2st)^y=[(s^2+t^2)^{z_1}+(s^2-t^2)^{x_1}][(s^2+t^2)^{z_1}-(s^2-t^2)^{x_1}]。\quad(10)$$

先设$2|x_1$，由于s,t均不含$4k+1$形素因子，故奇素数$p|s\Rightarrow p\nmid(s^2+t^2)^{z_1}+(s^2-t^2)^{x_1}$，奇素数$q|t\Rightarrow q\nmid(s^2+t^2)^{z_1}+(s^2-t^2)^{x_1}$，故注意到$(s^2+t^2)^{z_1}+(s^2-t^2)^{x_1}\equiv2(\mathrm{mod}4)$，由(10)得出

$$\begin{cases}(s^2+t^2)^{z_1}+(s^2-t^2)^{x_1}=2,\\(s^2+t^2)^{z_1}-(s^2-t^2)^{x_1}=2^{y-1}(st)^y。\end{cases}$$

而这显然不成立。于是$2\nmid x_1$，可设$x_1=2x_2+1$，$x_2\geqslant0$，与在$2|x_1$时同样讨论知，(10)给出

$$\begin{cases}(s^2+t^2)^{z_1}+(s^2-t^2)^{2x_2+1}=2^{y-1}s^y\\(s^2+t^2)^{z_1}-(s^2-t^2)^{2x_2+1}=2t^y,\end{cases}$$

或

$$\begin{cases}(s^2+t^2)^{z_1}+(s^2-t^2)^{2x_2+1}=2s^y,\\(s^2+t^2)^{z_1}-(s^2-t^2)^{2x_2+1}=2^{y-1}t^y。\end{cases}$$

然后在定理所设条件下，利用不等式法证明仅有 $y=2$ 的正整数解。

1962年，陈景润[36]用柯召的方法又补充了定理 5 和定理 6 中的某些结果。1982年，曹珍富[37]证明了：设$s=2n$和t均不含有$4k+1$形素因子，$t\not\equiv5(\mathrm{mod}8)$。则在

1） $n\equiv1(\mathrm{mod}6)$，$t\equiv1(\mathrm{mod}3)$时，或

2） $n\equiv5(\mathrm{mod}6)$，$t\equiv2(\mathrm{mod}3)$时，

Jeśmanowicz猜测成立。

显然，柯召、陈景润等对（9）中的商高数组的工作，都是在"s,t均不含有$4k+1$形素因子"的限制下进行的。1982

年，曹珍富[38]在许多情形下去掉了这个限制，得到

定理 7 设$s\equiv 2(\bmod 4)$，$t\equiv 1(\bmod 4)$，或$s\equiv 2(\bmod 4)$，$t\equiv 3(\bmod 4)$ 且$s+t$ 含有某个 $4k-1$ 形的素因子，则 Jeśmanowicz猜测成立。

定理 8 设

1） $s\equiv 1(\bmod 4)$，$t\equiv 2(\bmod 4)$，且s含有某个$4k-1$形的素因子或存在某个$8k+5$形状的素数 p适合同余式 $s^2\equiv t^2(\bmod p)$，或

2） $s\equiv 5(\bmod 8)$，$t\equiv 2(\bmod 8)$，或

3） $s\equiv 1(\bmod 8)$，$t\equiv 6(\bmod 8)$，或

4） $s\equiv 3(\bmod 4)$，$t\equiv 2(\bmod 4)$，且$s+t$ 含有某个$4k-1$形的素因子，则Jeśmanowicz猜测成立。

§3 与有限单群相关的指数丢番图方程

现在我们来考虑方程

$$1+p^a=q^br^c+p^dq^er^f \tag{1}$$

的非负整数解，这里p,q,r 是给定的不同素数。这个方程很自然地出现在有限单群中，例如

设G是一个有限单群，G 的阶 $|G|=pm$，p是素数且$(p,m)=1$，则在G的主p —块中寻常不可约特征标的次数$x_1,\cdots,x_n$满足如下形式的方程

$$\sum_{i=1}^{n}\delta_i x_i=0,\ \delta_i\in\{-1,1\}\quad(i=1,\cdots,n), \tag{2}$$

这里$x_1\cdots x_n$是$|G|/p$中一些素数幂的乘积。

显然，方程(1)是方程(2)在$n=4$且 $x_1\cdots x_4=p^uq^vr^w$ 时的一个情形。

对于某些特殊的有限单群G，例如G使得对某个Sylow p—子群S_p有$|N(S_p)|=3p$。由Brauer[39]的工作知，G的主p—块$B_0(p)$中的诸特征标是主特征标1，两个非例外特征标Λ，Γ和$\frac{p-1}{2}$个例外特征标$\chi^{(m)}(m=1,\cdots,\frac{p-1}{2})$。这些特征标对于符号$\delta_1$，$\delta_2$，$\delta'\in\{-1,1\}$满足$\Lambda(1)\equiv\delta_1(\bmod p)$，$\Gamma(1)\equiv\delta_2(\bmod p)$，$\chi^{(m)}(1)\equiv-3\delta'(\bmod p)(m=1,\cdots,\frac{p-1}{2})$和

$$1+\delta_1\Lambda(1)+\delta_2\Gamma(1)+\delta'\chi^{(m)}(1)=0。$$

故在假定$B_0(p)$有次数方程

$$1+2^a=3^b5^c+2^d3^e5^f \tag{3}$$

时，这里a,b,c,d,e,f均是非负整数，利用方程(3)的解可证[40]此时G与群$L(2,7)$，$U(3,3)$，$L(3,4)$或A_8之一同构。

1985年，Alex[41]给出了方程(1)在$\{p,q,r\}=\{2,3,5\}$时的全部非负整数解。易知，在$\{p,q,r\}=\{2,3,5\}$时，方程(1)化为方程(3)和方程

$$1+3^a=2^b5^c+2^d3^e5^f, \tag{4}$$

$$1+5^a=2^b3^c+2^d3^e5^f。 \tag{5}$$

定理 1 方程(3)的全部非负整数解为$(a,b,c,d,e,f)=$(3,0,1,2,0,0)，(5,0,2,3,0,0)，(6,0,2,3,0,1)，(7,0,3,2,0,0)，(10,0,4,4,0,2)，(10,0,2,3,0,3)，(2,1,0,1,0,0)，(3,1,0,1,1,0)，(4,2,0,3,0,0)，(5,3,0,1,0,0)，(5,2,0,3,1,0)，(7,4,0,4,1,0)，(9,4,0,4,3,0)，(9,3,0,1,5,0)，(6,1,1,1,0,2)，(9,5,0,1,3,1)，(6,0,1,2,1,1)，(12,0,5,2,5,0)，(6,2,1,2,0,1)，(9,2,2,5,2,0)，(9,4,1,2,3,0)，(7,2,0,3,1,1)，(4,0,1,2,1,0)，(10,0,3,2,2,2)，(10,2,2,5,0,2)，(4,1,1,1,0,0)，(7,1,2,1,3,0)，(11,4,2,3,

1,0,), (8,2,2,5,0,0), (5,1,0,1,1,1), (5,1,1, 1,2,0)和(t,0,0,t,0,0)，这里t是任意非负整数。

定理 2 方程(4)的全部非负整数解为 (2,0,1,0,0,1), (3,0,2,0,1,0), (2,3,0,1,0,0), (4,6,0,1,2,0), (3,3,0, 2,0,1), (5,6,0,2,2,1), (4,1,1,3,2,0), (6,1,1,4,2,1), (2,1,0,3,0,0), (6,7,1,1,2,1), (1,1,0,1,0,0), (3,1,1, 1,2,0), (4,1,0,4,0,1), (4,4,1,1,0,0), (6,1,3,5,1,1), (3,4,0,2,1,0), (4,1,2,5,0,0), (3,2,1,3,0,0), (3,2,0, 3,1,0), (2,2,0,1,1,0), (8,8,2,1,4,0), (4,5,0,1,0,2), (5,2,0,4,1,1), (5,2,2,4,2,0), (t,0,0,0,t,0),这里t是任意非负整数。

定理 3 方程(5)的全部非负整数解为(1,0,1,0,1,0), (3,0,4,0,2,1), (2,3,0,1,2,0), (2,3,1,1,0,0),(4,6,2, 1,0,2), (3,3,2,1,3,0),(2,1,0,3,1,0), (3,1,1,3,1,1), (2,1,2,3,0,0), (3,1,3,3,2,0), (2,4,0,1,0,1), (5,10, 1,1,3,0),(5,1,3,10,1,0), (1,1,0,2,0,0), (2,1,1,2,0, 1), (3,1,2,2,3,0), (1,2,0,1,0,0), (3,5,1,1,1,1), (3, 2,2,1,2,1), (3,2,3,1,2,0)和 (t,0,0,0,0,t),这里t是任意非负整数。

这三个定理的证明都借助了CDC660 计算机，同时用到了Tijdeman的一个结果，即

定理 4 设p,q是素数且$1<p<q<20$，则不等式$0<|p^x-q^y|<p^{x/2}$仅有解是 $(p,q,x,y)=$(2,3,1,1), (2,3, 2,1), (2,3,3,2), (2,3,5,3), (2,3,8,5), (2,5,2,1),(2, 5,7,3), (2,7,3,1), (2,11,7,2), (2,13,4,1), (2,17,4, 1), (2,19,4,1), (3,5,3,2),(3,7,2,1), (3,11,2,1), (3, 13,7,3), (5,7,1,1), (5,11,3,2), (7,19,3,2), (11,13,

1,1)和(17,19,1,1)。

稍后，Alex[42]又在$\{p,q,r\}=\{2,3,7\}$时给出了方程(1)的全部非负整数解。

对于$r=2$，$(p,q)=(73,223)$或$(223,73)$，Alex和Foster[43]证明方程(1)仅有平凡解$(t,0,0,t,0,0)$，t为任意非负整数。同时他们还考虑了$p=2$的某些情形。

1986年，曹珍富和黎进香[44]进一步讨论了方程(1)当$r=2$的情形：

$$1+p^a=q^b2^c+p^dq^e2^f, \tag{6}$$

在$p\equiv 1 \pmod{12}$，$q\equiv 7 \pmod{12}$且$\left(\frac{q}{p}\right)=1$时，他们证明了方程(6)推出$c=e=f=0$，故此时(6)化为

$$1+p^a=q^b+p^d。 \tag{7}$$

显然，除去$a=d$，$b=0$外，可设$a>0$，$b>0$，$d>0$，这时对给定p,q，方程(7)可以按照下述方法求解：

1°求出p对模q的阶数u；

2°选取某些$j\mid q^b-1$使得p对模j有阶数v，且$u\nmid v$。

因为从(7)得出$u\mid a-d$且$v\mid a-d$，故由$u\nmid v$知，不可能。这就证明在1°，2°两条均达到时方程(7)仅有平凡解$a=d$，$b=0$。利用这种方法，我们证明了

定理 5 设$(p,q)=(13,43)$，$(13,79)$，$(13,103)$，$(37,7)$，$(37,67)$，$(61,19)$，$(61,43)$和$(61,103)$，则方程(6)均仅有平凡解$(t,0,0,t,0,0)$，这里t为任意非负整数。

此外，1976年Alex[45]给出了$1+y=z$，$yz=2^a3^b5^c7^d$ $(a,b,c,d$均为非负整数$)$的全部正整数解(y,z)，共23组；他还给出了

$x+y=z$，$xyz=2^a3^b5^c7^d$，$x<y$，$(x,y)=1$

的全部正整数解(x,y,z)，共62组。1982年，Brenner和Foster[46]研究了许多类型的指数丢番图方程，例如他们给出了方程

$$1+2^a+7^b=3^c+5^d, \tag{8}$$

$$3^a+7^b=3^c+5^d+2, \tag{9}$$

$$3^a+5^b+7^c=11^d \tag{10}$$

等的全部非负整数解，分别为：

(8)：$(a,b,c,d)=(1,0,1,0)$，$(1,1,2,0)$，$(1,2,3,2)$，$(2,0,0,1)$，$(3,0,2,0)$，$(5,0,2,2)$，$(5,2,4,0)$。

(9)：$(a,b,c,d)=(1,0,0,0)$，$(2,0,1,1)$，$(3,0,0,2)$，$(3,3,5,3)$，$(4,2,1,3)$，$(6,4,1,5)$，$(t,1,t,1)$，

这里t为任意的非负整数。

(10)：$(a,b,c,d)=(1,0,1,1)$，$(2,0,0,1)$。

1986年，Kutsuna[47]给出了方程

$$a^x-b^yc^z=\pm1,\ \pm2,$$

在$\{a,b,c\}=\{2,3,5\}$时的全部正整数解(x,y,z)。

这里讨论的所有丢番图方程都是方程(2)的特例。而对方程(2)的较为一般情形，哪怕对方程(1)的较为一般情形，给出进一步的结果都不容易。

§4 丢番图方程$x^2+D=p^n$

对给定$D\in Z$和素数p，$p\nmid D$，求丢番图方程

$$x^2+D=p^n \tag{1}$$

的正整数解x,n，是一个著名的问题。早在1913年，Ramanujan就提出求方程

$$x^2+7=2^n \tag{2}$$

的正整数解的问题，他问：方程(2)除开$(x,n)=(1,3),(3,4),(5,5),(11,7),(181,15)$外，是否还有其他的解？这个问题首先由 Nagell 给出肯定的回答。后来，Mordell，Hasse，Chowla和Lewis，以及Johnson[48]等分别给出了多种不同的证明。我们在第二章§7和第三章§1、3分别给出了Johnson和Hasse的证明。有趣的是，方程(2)的解完全解决了组合数学中超平面差集（$v=2^n-1$，$n\geq 2$）和Hall 差集($v=4x^2+27$是素数）有无公共部分的问题。

1960年，Apéry[49]证明了丢番图方程

$$x^2+D=2^n,\quad 2\nmid D>0 \qquad (3)$$

在$D\neq 7$时最多有两组正整数解x,n。Browkin和Schinzel[50]提出如下猜想：方程(3)有两组正整数解当且仅当$D=23$，或$D=2^k-1$，$k>3$。

1967年，Schinzel[51] 部分地解决了这个猜想，证明了

定理 1 除$D=2^k-1$外，方程(3)在$n>80$ 时最多只有一组正整数解。

1981年，Beukers[52]完全解决了Browkin-Schinzel 猜想，证明了

定理 2 方程(3)有两组正整数解的充要条件是$D=23$或$D=2^k-1$，$k>3$。并且$D=23$时的解为$(x,n)=(3,5),(45,11)$；$D=2^k-1(k>3)$时的解为$(x,n)=(1,k)$，$(2^{k-1}-1,2k-2)$。

证明 首先在$D\not\equiv -1(\mathrm{mod}\,8)$时，对(3)取模8知$n<3$，故此时(3)不可能有两组正整数解。

现设$D\equiv -1(\mathrm{mod}\,8)$。令$e$ 是满足$M^2+b^2D=2^{2+e}$（对正整数M,b)的最小正整数，则熟知[49]：如果存在整数 x,r满足$x^2+D=2^{2+r}$，则$b=1$且$e\mid r$。此外，对于由

$$a_0=0,\ a_1=1,\ a_m=Ma_{m-1}-2^e a_{m-2},\ m\geqslant 2 \qquad (4)$$

给出的Lucas序列(参阅§6)，我们有$|a_{r/e}|=1$。反过来，如果存在m使得$|a_m|=1$，则对某正整数x和$D=2^{2+e}-M^2$有$x^2+D=2^{2+me}$。这样，我们来寻找满足$|a_m|=1(m>1)$的Lucas序列(4)。

设$|a_m|=1$且$2|me$，则对某正整数x有$x^2+D=2^{2+me}$，于是由$2^{2+e}=M^2+b^2D>D=2^{2+me}-x^2>2^{2+\frac{me}{2}}-1$知$m\leqslant 2$，故方程 $x^2+D=2^n$的解由$|a_1|=1$和$|a_2|=1$ 分别给出$(x,n)=(1,\ 2+e)$和$(2^{e+1}-1,\ 2+2e)$。

设$|a_m|=1$且$2\nmid me$，这时仍推出对某正整数x，有 $x^2+D=2^{2+me}$。我们考虑D的两种情形：

1） $D<2^{96}$，由第三章§4 Ⅲ的 Beukers 定理可推出：对任意$D\in Z$，如果$|D|<2^{96}$，且$x^2+D=2^n$有解，则$n<18+2\dfrac{\log|D|}{\log 2}$。于是我们得出

$$2+me<18+2\frac{\log D}{\log 2}，$$ 又由$2^{2+e}=M^2+D$推出$e\geqslant \dfrac{\log D}{\log 2}-2$，故由$D\geqslant 7$ 得出

$$m<20\frac{\log 2}{\log\frac{D}{4}}+2<27。\qquad (5)$$

由$D\neq 7$，$D\equiv -1(\mathrm{mod}\,8)$易知$D=15,\ 23,\cdots$，分别讨论(注意把增大的$D$代入(5)式可使$m$的范围缩小）知均不可能。

2） $D>2^{96}$，此时由第三章 §4 的例4知 $2+me<435+10\dfrac{\log D}{\log 2}$，故由 $e\geqslant\dfrac{\log D}{\log 2}-2$推出

$$m < \frac{455}{\log\frac{D}{4}} \log 2 + 10 < 15。$$

$$e > 94。$$

从Lucas序列(4)用简单同余法知$a_m \equiv M^{m-1} \pmod{2^e}$，因此$a_m = 1$推出$M^{m-1} \equiv 1 \pmod{2^e}$。令$m = 1 + 2^{t+1}a$，$2 \nmid a$，由$m < 15$知$t \leqslant 2$。再由$M^{m-1} \equiv 1 \pmod{2^e}$得出$M^2 \equiv 1 \pmod{2^{e-t}}$。注意到$M^2 < 2^{2+e}$，可设$M^2 = 1 + 2^{e-t}\mu$，$0 \leqslant \mu \leqslant 2^{2+t} \leqslant 16$。

假定$M = 1$，用归纳法得出：对所有$m \geqslant 2$有

$$a_m \equiv 1 - (m-2)2^e \pmod{2^{2e}}。$$

因此$a_m = 1$推出$m - 2 \equiv 0 \pmod{2^e}$，但$2 \nmid m$，故这是不可能的。于是$M > 1$，令$M = \pm 1 + \rho \cdot 2^k$，$k \geqslant 2$，$2 \nmid e$，则有$1 \pm \rho \cdot 2^{k+1} + \rho^2 \cdot 2^{2k} = 1 + \mu \cdot 2^{e-t}$，即$\rho \cdot 2^{k+1}(\rho \cdot 2^{k-1} \pm 1) = \mu \cdot 2^{e-t}$。由此知$2^{e-t} \mid 2^{k+1}$，故得$k + 1 \geqslant e - t > 92$且$\rho(\rho \cdot 2^{k-1} \pm 1) \leqslant \mu$。因为$\mu < 16$，$k \geqslant 92$，所以$2^{91} - 1 \leqslant \rho(\rho \cdot 2^{k-1} \pm 1) \leqslant \mu \leqslant 16$，这是矛盾的。这就证明了定理2。证毕。

Beukers还同时讨论了方程

$$x^2 - D = 2^n, \quad 2 \nmid D > 0 \tag{6}$$

的解。显然

Ⅰ. 如果$D = 2^{2k} - 3 \cdot 2^{k+1} + 1$，$k \geqslant 3$，则方程(6)有解$(x, n) = (2^k - 3, 3)$，$(2^k - 1, k + 2)$，$(2^k + 1, k + 3)$，$(3 \cdot 2^k - 1, 2k + 3)$。

Ⅱ. 如果$D = 2^{2l} + 2^{2k} - 2^{k+l} - 2^{k+1} - 2^{l+1} + 1$，$k > 1$，$l \geqslant k + 1$，则方程(6)有解$(x, n) = (2^l - 2^k - 1, k + 2)$，$(2^l - 2^k + 1, l + 2)$，$(2^k + 2^l - 1, k + l + 2)$。

Ⅲ. 如果$D = \left(\frac{2^{l-2} - 17}{3}\right)^2 - 32$，$2 \nmid l \geqslant 9$，则方程(6)有

解$(x,n)=\left(\frac{2^{l-2}-17}{3},5\right)$，$\left(\frac{2^{l-2}+1}{3},\ l\right)$和$\left(\frac{17\cdot 2^{l-2}-1}{3},\ 2l+1\right)$。

一般地，有如下的定理。

定理 3 方程(6) 最多有四组正整数解，且除Ⅰ，Ⅱ和Ⅲ的情形外，方程(6)最多有三组正整数解。

如果$D<10^{12}$，则除Ⅰ，Ⅱ和Ⅲ外最多有两组解，而在Ⅰ，Ⅱ和Ⅲ时分别恰有四，三和三组正整数解。

对于$|D|<1000$，我们已知方程$x^2-D=2$ 有两个或多于两个正整数解的全体D和解如下：

D	(x,n)
$D=-511$，	$(x,n)=(1,9)$，$(255,16)$
-255，	$(1,8)$，$(127,14)$
-127，	$(1,7)$，$(63,12)$
-63，	$(1,6)$，$(31,10)$
-31，	$(1,5)$，$(15,8)$
-23，	$(3,5)$，$(45,11)$
-15，	$(1,4)$，$(7,6)$
-7，	$(1,3)$，$(3,4)$，$(5,5)$，$(11,7)$，$(181,15)$
17，	$(5,3)$，$(7,5)$，$(9,6)$，$(23,9)$
33，	$(7,4)$，$(17,8)$
41，	$(7,3)$，$(13,7)$
65，	$(9,4)$，$(33,10)$
89，	$(11,5)$，$(91,13)$
105，	$(11,4)$，$(13,6)$，$(19,8)$
113，	$(11,3)$，$(25,9)$
161，	$(13,3)$，$(15,6)(17,7)$，$(47,11)$

217,	(15,3), (27,9)
257,	(17,5), (129,14)
273,	(17,4), (23,8)
329,	(19,5), (29,9)
345,	(19,4), (37,10)
353,	(19,3), (49,11)
497,	(23,5), (25,7), (39,10)
513,	(23,4), (257,16)
665,	(27,6), (69,12)
697,	(27,5), (363,17)
713,	(27,4), (29,7), (35,9)
721,	(27,3), (183,15)
777,	(29,6), (131,14)
825,	(29,4), (43,10)
833,	(29,3), (31,7), (33,8), (95,13)
945,	(31,4), (71,12)

由此可见，Beukers对方程(1)当$p=2$时的研究已经十分完整。

对$p>2$，$D>0$，Apéry[53]证明了

定理 4 设$D>0$，p是奇素数，则方程(1)最多有两组正整数解。

1973年，Alter和Kubota[54]利用代数数论方法给出了方程

$$x^2+D=p^n，p\text{是奇素数}，p\nmid D>0 \tag{7}$$

在$D\equiv 3(\bmod 4)$，$D>3$无平方因子时有解的充要条件。Kutsuna[55]补充了Alter—Kubota的结果，例如在$D\equiv$

1(mod4)时，他证明了：设$2^t \| a$，$2^2 \| p-1$且对 $1 \leqslant r \leqslant \frac{t-1}{2}$ 有$p \not\equiv 2^t+1-2^{2r} \pmod{2^{2r+2}}$，则方程(7)最多有一组正整数解。

1979年，Beukers[56]对方程(7)作了系统的研究，例如他证明了

定理 5 设e是对于正整数a，b使得$a^2+Db^2=p^e$的最小正整数，且$\lambda=a+\sqrt{-D}$，$\bar{\lambda}=a-\sqrt{-D}$，如果(7)有解$(x,n)$，则1)$e \mid n$且$b=1$；2)$\frac{\lambda^{n/e}-\bar{\lambda}^{n/e}}{\lambda-\bar{\lambda}}=\pm 1$；3)$n/e$是奇数。

这个定理利用第三章§1的例5很容易证明。利用这个定理可以推出若干结果来。例如

Kutsuna[57]，乐茂华[58]等都得出过一些结果。由这些结果可知，在许多情形下方程(7)最多只有一组正整数解。

许多人对一些特殊的D和p值，给出了方程(7)的全部正整数解（其中有不少结果包含在第八章对方程$x^2+D=y^n$的讨论中）。

对于$p>2$，$D<0$，这时方程(1)化为

$$x^2+D=p^n,\ p\text{是奇素数},\ p \nmid D<0。\tag{8}$$

Beukers[59]在1981年证明了

定理 6 设$-D$不是平方数，如果方程(8)有两组解$(x,n)=(A,k)$，(A',k')，$k'>k$，则

$$p^k \leqslant \max(2\cdot 10^6,\ 600D^2)。$$

定理 7 方程(8)最多有四组正整数解。

最后，对于方程

$$x^2+D^m=p^n,\ p\text{是素数},\ p \nmid D,\tag{9}$$

其中D，p 是给定的，也有过许多工作。1979年，Toyoizumi[60]、[61]证明了

定理 8　设$D=2^{a+2}-a^2\neq 7$，a和D均是正整数，则方程

$$x^2+D^m=2^n$$

推出$m=1$。

定理 9　设$D>1$无平方因子，$p\equiv 3\pmod 4$，如果$D\equiv 1,\ 2\pmod 4$且$p-D$是一个平方数，则除$(D,p)=(2,3)$外方程(9)推出$m=1$。

对D和p取一些特殊值时，Yamabe[62]、[63]和Kutsuna[64]还有一些工作。孙琦与曹珍富[65]用初等方法还给出了方程(9)的较为一般的解答。

§5　方程 $x^xy^y=z^z$ 及其推广

Erdös曾经猜想：方程

$$x^xy^y=z^z,\quad x>1,\quad y>1,\quad z>1 \tag{1}$$

无整数解x,y,z。1940年，柯召[66]否定了这个猜想，给出了方程(1)的无穷多组解

$$\begin{aligned} x&=2^{2^{n+1}(2^n-n-1)+2n}(2^n-1)^{2(2^n-1)}\\ y&=2^{2^{n+1}(2^n-n-1)}(2^n-1)^{2(2^n-1)+2}\\ z&=2^{2^{n+1}(2^n-n-1)+n+1}(2^n-1)^{2(2^n-1)+1}\end{aligned} \tag{2}$$

这里$n>1$。同时，他证明了$(x,y)=1$时，方程(1)无解。

1958年，Schinzel[67]证明了：如果方程(1)有解，则x的每一个素因子整除y，或y的每一个素因子整除x。这一结果的证明是十分容易的，例如阎发湘[68] 给出的证明如下：

不妨设$x<y$且$p|x$但$p\nmid y$。于是可令

$$p^{\alpha}\| x,\ p^{\beta}\| z,\ \alpha>0,\ \beta>0,$$

由方程(1)得出$\alpha x=\beta z$，从而$p^{\alpha-\beta}|\beta$，即$p^{\beta(\frac{z}{x}-1)}\Big|\beta$，由此推出 $z\leqslant\frac{3}{2}x$。令$y=x+y_2$，$y_2\geqslant1$，由(1) 式得出

$x^{\frac{1}{2}x+1}<\left(\frac{3}{2}\right)^{\frac{3}{2}x}$，但这是不可能的。

Schinzel猜想：在方程(1)的解中，x与y有相同的素因子。1975年，Dem′janenko[69]证明了这个猜想，即有

定理 1 设x,y,z是方程(1)的解，则x,y有相同的素因子。

另一方面，Mills[70]在1959年发现柯召得到的解中x，y，z均满足关系$4xy=z^2$，于是他对$4xy>z^2$，$4xy=z^2$进行了研究，证明了

定理 2 如果$4xy>z^2$，则方程(1)无解；如果$4xy=z^2$，则方程(1)仅有正整数解(2)。

1984年，Uchiyama[71] 研究了$4xy<z^2$的情形，证明了在$4xy<z^2$时方程(1)最多只有有限组解。

很可能(2)给出了方程(1)的全部解。

对于方程(1)的推广，即丢番图方程

$$\prod_{i=1}^{k}x_i^{x_i}=z^z,\ k\geqslant2,\ x_i>1(i=1,\cdots,k),\tag{3}$$

在1964年，柯召和孙琦[87]首先证明了

定理 3 方程(3)有无穷多组解

$$x_1=k^{A_1+2n}(k^n-1)^{B_1},$$

$$x_2=k^{A_1}(k^n-1)^{B_1+2},$$

$$x_3 = \cdots = x_k = k^{A_1+n}(k^n-1)^{B_1+1},$$

$$z = k^{A_1+n+1}(k^n-1)^{B_1+1},$$

这里$A_1 = k^n(k^{n+1}-2n-k)$，$B_1 = 2(k^n-1)$，而k,n满足$k=2$时$n>1$，$k\geqslant 3$时$n>0$。（证明见第二章§8）。

利用Schinzel引理，即如果正整数a_1，a_2，b_1,b_2,b_3满足$a_1^{a_1a_2} = b_1^{b_1b_2b_3}$，$(a_1, b_2b_3) = (a_2, b_1b_3) = 1$,$a_1>1$，$b_1b_2b_3 \geqslant a_1a_2$，则$b_1>b_3$。他们还证明了

定理 4 设方程(3)有解$x_i(i=1,\cdots,k)$，则至少存在一个j，$1\leqslant j\leqslant k$，使x_j的每一个素因子整除$\prod_{\substack{i=1\\i\neq j}}^{k} x_i$。

由此可知，方程(3)在$x_1,\cdots,x_k$两两互素时无解。

阎发湘[72]改进了定理4得到如下的结果。

定理 5 设方程(3)有解$x_i(i=1,\cdots,k)$，则最多存在一个j，$1\leqslant j\leqslant k$，使x_j有与$\prod_{\substack{i=1\\i\neq j}}^{k} x_i$互素的因子$v_j>1$。

证 否则，可设有另一个$x_l(l\neq j)$，有与$\prod_{\substack{i=1\\i\neq l}}^{k} x_i$互素的因子$v_l>1$，且不妨设$v_l$是$x_l$与$\prod_{\substack{i=1\\i\neq l}}^{k} x_i$互素的最大因子，相应地设$v_j$是$x_j$与$\prod_{\substack{i=1\\i\neq j}}^{k} x_i$互素的最大因子。令

$$r_j = \frac{x_j}{v_j}, \qquad r_l = \frac{x_l}{v_l}, \qquad r = \frac{z}{z_j \cdot z_l},$$

这里z_j，z_l分别是z与$\prod_{\substack{i=1\\i\neq j}}^{k} x_i$以及$z$与$\prod_{\substack{i=1\\i\neq l}}^{k} x_i$互素的最大因

子。于是由(3)得

$$v_l^{v_l r_l} r_l^{v_l r_l} v_j^{v_j r_j} r_j^{v_j r_j} \prod_{\substack{i=1 \\ i \neq j,\, l}}^{k} x_i^{x_i}$$

$$= z_l^{z_l z_j r} z_j^{z_l z_j r} r^{z_l z_j r},$$

这给出

$$v_l^{v_l r_l} = z_l^{z_l z_j r}, \tag{4}$$

$$v_j^{v_j r_j} = z_j^{z_l z_j r}, \tag{5}$$

由于$(v_l,\ rz_j)=(r_l,\ z_l z_j)=1$，及

$$z_l z_j r \geqslant v_l r_l,\quad v_l > 1,$$

$$(v_j,\ rz_l)=(r_j,\ z_l z_j)=1,$$

$$z_l z_j r \geqslant v_j r_j,\quad v_j > 1,$$

故由(4)，(5)均满足Schinzel引理，得

$$z_l > z_j \text{ 以及 } z_j > z_l,$$

这是矛盾结果。证毕。

1983年，姚兆栋[73] 利用柯召和孙琦的方法（见第二章§8），又给出了方程(3)的一些解，特别是给出了方程(3)在$2|k\geqslant 4$时的奇数解。

定理 6 方程(3)在$k\geqslant 3$时有解

$$x_1 = 2^{2n(2^{k-2}-1)},\quad x_2 = 2^{2n(2^{k-2}-1)} n,$$

$$x_i = 2^{2n(2^{k-2}-1)+i-3} n \ (i=3,\cdots,k),$$

$$z = 2^{2n(2^{k-2}-1)+k-2} n,$$

这里n是正整数。

定理 7 方程(3)有解

$$x_1 = 2^{A_2+2n}(2^n-1)^{B_2},\quad x_2 = 2^{A_2}(2^n-1)^{B_2+2},$$

$$x_i = 2^{A_2+i-2}(2^n-1)^{B_2+1} \ (i=3,\cdots,k),$$

$$z=2^{A_2+n+k-1}(2^n-1)^{B_2+1}$$

这里$A_2=2^{n+1}[(2^{k-1}-1)(2^{n-1}-1)-n]$, $B_2=2(2^n-1)$，且$k=2$时$n>1$，$k\geqslant 3$时$n\geqslant 1$。

定理 8 设$k\geqslant 3$，则方程(3)有解

$$x_i=(k-m)^{n(k-m)}\quad(i=1,\cdots,m),$$
$$x_j=m\cdot n(k-m)^{n(k-m)}\quad(j=m+1,\cdots,k)$$
$$z=mn(k-m)^{n(k-m)+1},$$

这里$k>m\geqslant 1$。

由定理8知，在$2|k\geqslant 4$时方程(3)有无穷多组奇数解（只要在定理8中取$2|k$，$2\nmid mn$即得）。

为了证明这些定理，设$(x_1, x_2,\cdots,x_k,z)=d$，令$x_i=dt_i(i=1,\cdots,k)$，$z=du$，代入(3)得

$$d^{\sum_{i=1}^{k}t_i-u}\prod_{i=1}^{k}t_i^{t_i}=u^u,$$

由此知，满足条件

$$\begin{cases}\sum_{i=1}^{k}t_i-u=r, & (6)\\ \dfrac{u^u}{\prod_{i=1}^{k}t_i^{t_i}}\text{为正整数的}r\text{次幂}(=d^r), & (7)\end{cases}$$

这里$r\geqslant 1$为整数，的$t_i(i=1,\cdots,k)$和u可给出方程(3)的解。

令$t_1=1$，$t_2=n$，$t_i=2^{i-3}n(i=3,\cdots,k)$, $u=2^{k-2}n$，代入(6)、(7)式得出$r=1$，$d=2^{2n(2^{k-2}-1)}$，故给出定理6的解。

令$t_1=2^{2n}$，$t_2=(2^n-1)^2$，$t_i=2^{n+i-2}(2^n-1)(i=3,\cdots,k)$，$u=2^{n+k-1}(2^n-1)$，代入(6)、(7)式得出$r=1$，

$d=2^{A_2}(2^n-1)^{B_2}$，这里

$A_2=2^{n+1}[(2^{k-1}-1)(2^{n-1}-1)-n], B_2=2(2^n-1)$。
故得出定理7中的解。

令$t_i=1\ (i=1,\cdots,m)$，$t_j=mn(j=m+1,\cdots,k)$，
$u=mn(k-m)$，代入(6)、(7)得出$r=m$，$d=(k-m)^{n(k-m)}$，
故给出定理8中的解。

利用这种构造方法，还可以给出方程(3)的许多解来。例如瞿维建[74]取$t_i=k^{2n}(i=1,\cdots,r)$，$t_j=(k^n-1)^2(j=r+1,\cdots,2r)$，$t_l=k^n(k^n-1)(l=2r+1,\cdots,k)$，
$u=k^{n+1}(k^n-1)$代入(6)、(7)得出

$$d=k^{\frac{k^{n+1}(k^n-1)}{r}-2nk^n}(k^n-1)^{2(k^n-1)},$$

故得

定理 9 对每个正整数 $r\leqslant\frac{k}{2}$，(3)有解

$$x_i=k^{A_3+2n}(k^n-1)^{B_3}\ (i=1,\cdots,r),$$

$$x_j=k^{A_3}(k^n-1)^{B_3+2}\ (j=r+1,\cdots,2r)$$

$$x_l=k^{A_3+n}(k^n-1)^{B_3+1}(l=2r+1,\cdots,k),$$

$$z=k^{A_3+n+1}(k^n-1)^{B_3},$$

这里$A_3=\frac{k^{n+1}(k^n-1)}{r}-2nk^n$，$B_3=2(k^n-1)$，

$k^{n+1}(k^n-1)\equiv 0(\bmod r)$，且$k=2$时$n>1$；$k>2$时$n>0$。

显然$k=2$时给出柯召得到的方程(1)的解。

取$t_i=2^{2n}(i=1,\cdots,r)$, $t_j=(2^n-1)^2(j=r+1,\cdots,2r)$, $t_l=2^{n+l-2r}(2^n-1)r(l=2r+1,\cdots,k)$, $u=2^{n+k-2r+1}(2^n-1)r$，于是(6)成立，(7)给出

$$d=2^{A_4}(2^n-1)^{B_4}r^{C_4},$$

这里$A_4=2^{n+1}[(2^{k-2r+1}-1)(2^n-1)-n]$,$B_4=2(2^n-1)$,$C_4=2^{n+1}(2^n-1)$。这就得到

定理10 对每个正整数 $r\leqslant\frac{k}{2}$,(1)有解

$$x_i=2^{A_4+2n}(2^n-1)^{B_4}r^{C_4}\ (i=1,\cdots,r),$$

$$x_j=2^{A_4}(2^n-1)^{B_4+2}r^{C_4}\ (j=r+1,\cdots,2r),$$

$$x_l=2^{A_4+n+l-2r}(2^n-1)^{B_4+1}r^{C_4+1}\ (l=2r+1,\cdots,k),$$

$$z=2^{A_4+n+k-2r+1}(2^n-1)^{B_4+1}r^{C_4+1},$$

这里$n>1$。

在 $2\nmid k\geqslant5$ 时，瞿维建构造了方程(3)的无穷多组奇数组，他的构造如下：

在$k=4m+1$，$m\geqslant1$时，取$t_1=3^{2n}$，$t_2=(3^n-2)^2$，$t_3=3^n(3^n-2)$，$t_{2i}=t_{2i+1}=3^{n+i-1}(3^n-2)(i=2,3,\cdots,2m)$，$u=3^{n+2m}(3^n-2)$，代入(6)、(7)得$r=4$，$d=3^{A_5}(3^n-2)^{B_5}$，这里$A_5=3^{n+1}\left(\frac{3^{2m}-1}{8}\right)(3^n-2)-n3^n$，$B_5=3^n-2$。于是得到

定理11 设$k=4m+1$，$m\geqslant1$，则方程(3)有解

$$x_1=3^{A_5+2n}(3^n-2)^{B_5},\quad x_2=3^{A_5}(3^n-2)^{B_5+2}$$

$$x_3=3^{A_5+n}(3^n-2)^{B_5+1}$$

$$x_{2i}=x_{2i+1}=3^{A_5+n+i-1}(3^n-2)^{B_5+1}\ (i=2,3,\cdots,2m),$$

$$z=3^{A_5+n+2m}(3^n-2)^{B_5+1},$$

这里n是正整数。

在$k=4m+3$，$m\geqslant 1$时，取$t_1=1$，$t_2=3^{2n}$，$t_3=3^{2n+1}$，$t_4=(2\cdot 3^n-1)^2$，$t_5=t_6=3^n(2\cdot 3^n-1)$，$t_7=3^{n+1}(2\cdot 3^n-1)$，$t_{2i}=t_{2i+1}=3^{n+i-2}(2\cdot 3^n-1)(i=4,5,\cdots,2m+1)$，$u=3^{n+2m}(2\cdot 3^n-1)$，代入(6)、(7)式得$r=4$，$d=3^{A_6}(2\cdot 3^n-1)^{B_6}$，这里$A_6=3^{n+1}\left[\left(\frac{3^{2m}-1}{4}\right)(2\cdot 3^n-1)+\frac{3^n-1}{2}\right]-2n\cdot 3^n$，$B_6=2\cdot 3^n-1$，故得

定理12 设$k=4m+3$，$m\geqslant 1$，则方程(3)有正整数解

$$x_1=3^{A_6}(2\cdot 3^n-1)^{B_6},\quad x_2=3^{A_6+2n}(2\cdot 3^n-1)^{B_6},$$

$$x_3=3^{A_6+2n+1}(2\cdot 3^n-1)^{B_6},\quad x_4=3^{A_6}(2\cdot 3^n-1)^{B_6+2},$$

$$x_5=x_6=3^{A_6+n}(2\cdot 3^n-1)^{B_6+1},\quad x_7=3^{A_6+n+1}(2\cdot 3^n-1)^{B_6+1},$$

$$x_{2i}=x_{2i+1}=3^{A_6+n+i-2}(2\cdot 3^n-1)^{B_6+1}\quad (i=4,5,\cdots,2m+1),$$

$$z=3^{A_6+n+2m}(2\cdot 3^n-1)^{B_6+1},$$

这里n为正整数。

由定理8,11和12立得

推论 在$k\geqslant 4$时方程(3)有奇数解。

但是，我们不知道$k=3$时方程(3)是否有奇数解（参阅第二章§8）。

最后指出，给出丢番图方程

$$x^y y^x=z^z,\quad x^y y^z=z^x,\quad x^x y^z=z^y$$

的一些解是容易的[68,75,76]，但给出它们的全部解仍很困难。

§6 其他一些指数丢番图方程。

本节我们讨论两类指数丢番图方程。

Ⅰ. 丢番图方程$x^2=4q^{a/2}+4q+1$

丢番图方程

$$x^2=4q^{a/2}+4q+1, \tag{1}$$

（这里x, a是正整数，q是一个素数的幂）是Calderbank[77]从编码理论中提出来的。例如他证明了

定理 1 设有限域$GF(q)$（q是一个素数幂）上的$[n, k]$码C恰有两个非零加权W_1，W_2，且在二重码$C^{\perp}$中最小加权至少是4。如果$k=2$，则$n=1$，$W_1=1$，$W_2=2$；

（A）如果$k\geqslant 3$，$q=2$，则下列两条之一成立：

1）$n=2^{k-1}$，$W_1=2^{k-2}$，$W_2=2^{k-1}$；

2）$k=4$，$n=5$，$W_1=2$，$W_2=4$。

（B）如果$k\geqslant 3$，$q\neq 2$，则

3）$k=3$，$q=2^m$，$n=2^m+2$，$W_1=2^m$，$W_2=2^m+2$；

4）$k=4$，$n=q^2+1$，$W_1=(q-1)q$，$W_2=q^2$；

5）$(q-1)n=u(q^{k/2}+1)$，$W_1=uq^{(k-2)/2}$，

$W_2=(u+1)q^{(k-2)/2}$，

这里u是一个正整数且$(2u+3)^2=4q^{k/2}+4q+1$，

或

6）$2(q-1)n=(2u+1)q^{(k-1)/2}+(q-2)-u(u+1)/q$，$W_1=uq^{(k-3)/2}$，$W_2=(u+1)q^{(k-3)/2}$，这里$u$是一个正整数，且$(2u+(2q+1))^2=4q^{(k+1)/2}+4q+1$。

由这个定理可见，给出方程(1)的全部解十分必要(Calderbank[77]对此曾作了一个猜想)。下面我们就来研究方程(1)的解。首先，如$2|a$，则方程(1)化为

$$x^2=4q^m+4q+1,\ m>0,\ x>0, \tag{2}$$

并且如果$2\nmid a$，则方程(1)化为

$$x^2=4q^m+4q^2+1,\ 2\nmid m>0,\ x>0。 \tag{3}$$

显然，对任给的q，(2)和(3)均分别有平凡解$m=2$，$x=2q+1$和$m=1$，$x=2q+1$。

对$q=3$，方程(2)化为$x^2=4\cdot 3^m+13$。Bremner等[78,79]以及Tzanakis和Wolfskill[80]证明了该方程仅有正整数解$(x,m)=(5,1),(11,3)$。对$q=4$，方程(1)化为$x^2=2^{2+a}+17$，此由§4知仅有正整数解$(x,a)=(5,1)$，$(7,3)$，$(9,4)$，$(23,7)$。

1987年，Tzanakis和Wolfskill[81]彻底解决了方程(2)和(3)，证明了

定理 2 设q是一个素数幂，则方程(2)仅有非平凡解$q=3$，$(x,m)=(5,1)$，$(11,3)$。方程(3)仅有非平凡解$q=2$，$(x,m)=(5,1)$，$(7,3)$，$(23,7)$。

由这个定理立即推出

推论 设C满足定理1的条件，则k,n,W_1和W_2仅有下列的可能值：

1)对任意q：$k=2$，$n=2$，$W_1=1$，$W_2=2$；

$k=4$，$n=q^2+1$，$W_1=(q-1)q$，$W_2=q^2$。再加上

2) $q=2$：$n=2^{k-1}$，$W_1=2^{k-2}$，$W_2=2^{k-1}$。

3) $q=3$：$k=5$，$n=11$，$W_1=6$，$W_2=9$；

$k=6$，$n=56$，$W_1=1$，$W_2=2$。

4) $q=4$：$k=6$，$n=78$，$W_1=56$，$W_2=64$；

$k=7$，$n=430$，$W_1=320$，$W_2=352$。

5） $q=2^m$：$k=3$，$n=2^m+2$，$W_1=2^m$，$W_2=2^m+2$。

至于定理2的证明，首先使用第三章§4Ⅲ的函数$G(z)$，$H(z)$，得到

$$\binom{n}{n_2}G(4z)-\binom{n}{n_2}\sqrt{1-4z}\,H(4z)$$

$$=(4z)^{n+1}\binom{n}{n_2}G(1)E(4z)=z^{n+1}E_1(z),$$

这里$E_1(z)$是z的幂级数。于是由 p-adic 知识（见第三章§3），令$q=p^f$，p是素数，$f>0$，则有

$$\left|\binom{n}{n_2}G(-4q)-\binom{n}{n_2}\sqrt{1+4q}\,H(-4q)\right|_p\leqslant|q^{n+1}|_p$$

$$=q^{-(n+1)} \tag{4}$$

其中$n=n_1+n_2$。对方程(2)（可设$m\geqslant3$），我们有

$$1+4q=x^2\left(1-\frac{4q^m}{x^2}\right),$$

不妨设$x\equiv1(\bmod p)$（因为由(2)知$x^2\equiv1(\bmod p)$），则上式给出

$$\sqrt{1+4q}=x\sqrt{1-\frac{4q^m}{x^2}}=x+q^m\xi,\ \xi\in Z_p, \tag{5}$$

这里Z_p是p-adic整环。因为x是p-adic单位，故从(4)，(5)得

$$|\lambda-x\eta-q^m\eta\xi|_p\leqslant q^{-(n+1)},$$

这里 $\lambda=\binom{n}{n_2}G(-4q)$，$\eta=\binom{n}{n_2}H(-4q)$。由于

$$|\lambda-x\eta|_p\leqslant\max(|\lambda-x\eta-q^m\eta\xi|_p,\ |q^m\eta\xi|_p)$$

$$\leqslant\max(q^{-(n+1)},q^{-m}),$$

因此$|\lambda-x\eta|_p\leqslant q^{-t}$，$t=\min\{m,n+1\}$。设$K=\lambda-x\eta$，则$K\in Z$，且$q^t|K$。易知$K\neq0$，故$|K|\geqslant q^t$。利用第三章§4Ⅲ

的知识还可以给出

$$\binom{n}{n_2}|H(z)|<\sum_{k=0}^{n_2}\binom{n_1}{k}\binom{n-k}{n_1}|z|^k$$

$$=\sum_{k=0}^{n_2}\binom{n_2}{k}\binom{n-k}{n_2}|z|^k\leqslant\binom{n}{n_2}(1+|z|)^{n_2},$$

故由$|x|<2q^{m/2}+1$得出

$$|K|<\binom{n}{n_2}[(1+4q)^{n_1}+(2q^{m/2}+1)(1+4q)^{n_2}]。$$

由此并注意到$|K|\geqslant q^t$，可推出$q<1000$。

类似的方法可以证明(3)在$m\geqslant 5$时推出$q<40$。

然后利用简单同余法，筛选掉一些q值，对剩下的q值，挨个使用递推序列法（见第二章§7和第七章§4）最终证明定理2。

对于丢番图方程

$$x^2=4q^n-4q+1,\ q是素数,$$

当$q=2$时退化为Ramanujan—Nagell方程（见§4），而当$q>2$时，Johnson[82]宣布，用递推序列法已给出解答。

Ⅱ. 丢番图方程$\alpha^n+\beta^n=2x^2$

设D不是平方数，$\alpha=a+b\sqrt{D}$，$\beta=a-b\sqrt{D}\in Q(\sqrt{D})$，这里$a,b\neq 0$是有理整数。我们来研究丢番图方程

$$\alpha^n+\beta^n=2x^2 \tag{6}$$

的正整数解x,n。

先首，在$N(\alpha)=1$时，柯召和孙琦[83]证明了方程(6)在$4|n$时无正整数解x,n。而在$N(\alpha)=-1$时，曹珍富[84]证明了类似的结论。由此知，在$N(\alpha)=\pm 1$时，方程

$$\alpha^{4m}+\beta^{4m}=2x^2 \tag{7}$$

无正整数解x,m。

1986年，孙琦[85]对方程(7)，考虑了$N(\alpha)=k$，$|k|>1$的情形，证明了

定理 3 设$N(\alpha)=k$，$|k|>1$，k满足以下条件：

1） k无平方因子；

2） k的任一个素因子p满足$p\nmid \Delta$，这里Δ是$Q(\sqrt{D})$的基数；

3） k至少含一个形如$8f+3$或$8f+5$的素因子q，则方程(7)无正整数解。

曹珍富[86]改进了这个结果，对方程

$$\alpha^{2m}+\beta^{2m}=2x^{2}, \tag{8}$$

证明了

定理 4 设$N(\alpha)=k$，$|k|>1$，如果存在某个$8f+3$或$8f+5$形的素数q，满足$q\| k$且$q\nmid \Delta$，这里Δ是$Q(\sqrt{D})$的基数，则方程(8)无正整数解。

证 设方程(8)有正整数解x，m，令$y=\dfrac{\alpha^{m}+\beta_{m}}{2}$，显然$y$是有理整数，由(8)给出

$$t^{2}=2y^{2}-k^{m}。 \tag{9}$$

由$q\| k$，对(9)取模q得

$$t^{2}\equiv 2y^{2}(\mathrm{mod}\,q)。 \tag{10}$$

由于q是$8f+3$或$8f+5$形的素数，故当$q\nmid y$时，(10)给出矛盾结果$\left(\frac{2}{q}\right)=1$，而当$q\mid y$时，由

$$y=\frac{\alpha^{m}+\beta^{m}}{2}=\sum_{i=0}^{m}\frac{1+(-1)^{i}}{2}\binom{m}{i}a^{m-i}(b\sqrt{D})^{i}$$

$$=\sum_{\substack{0\leqslant i\leqslant m\\ 2\mid i}}\binom{m}{i}a^{m-i}(b\sqrt{D})^{i}=\sum_{0\leqslant i\leqslant u}\binom{m}{2i}a^{m-2i}(b\sqrt{D})^{2i},$$

其中

$$u=\begin{cases}\dfrac{m-1}{2}, & \text{当}2\nmid m\text{ 时；}\\ \dfrac{m}{2}, & \text{当}2\mid m\text{ 时。}\end{cases}$$

及$a^2-Db^2=k\equiv 0(\bmod q)$知

$$0\equiv\sum_{0\leqslant i\leqslant u}\binom{m}{2i}a^{m-2i}a^{2i}=a^m\sum_{0\leqslant i\leqslant u}\binom{m}{2i}(\bmod q)。\quad(11)$$

现在我们来证明$q\nmid a^m$。不然设$q\mid a^m$，则$q\mid a$。由$a^2-Db^2=k$知$q\mid Db^2$。又由$q\nmid \varDelta$，$\varDelta=D$或$4D$知$q\mid b^2$，即$q\mid b$。由$q\mid a$，$q\mid b$及$a^2-Db^2=k$推出$q^2\mid k$，与$q\| k$矛盾。于是$q\nmid a^m$，(11)式给出

$$\sum_{0\leqslant i\leqslant u}\binom{m}{2i}\equiv 0(\bmod q),$$

但这是不可能的（因为

$$\sum_{0\leqslant i\leqslant u}\binom{m}{2i}=\frac{(1+1)^m+(1-1)^m}{2}=2^{m-1}）。\text{证毕。}$$

显然，如果在与定理4 的某些条件相重叠时，能够证明方程(6)无 $2\nmid n$ 的解，则方程(6) 对任何n都无正整数解。这对于方程(6)的具体应用来说是需要的。为此，我们证明了

定理 5 设 $\alpha=a+b\sqrt{D}$，$a>0$非平方数，$N(\alpha)=k$，$|k|>1$且k满足以下的条件：

1） $k\equiv 1(\bmod 4)$无平方因子且k含有 $8f+3$或 $8f+5$ 形的素因子；

2） k的任一素因子$p\nmid\varDelta$，$\varDelta$为$Q(\sqrt{D})$ 的基数，则方程(6) 无正整数解。

这个定理的证明需要研究

$$E(p)=\frac{\alpha^{pm}+\beta^{pm}}{\alpha^m+\beta^m}$$

的性质，这里p为奇素数，m为正整数。在定理5的条件下，$E(p)\equiv 1 \pmod 4$，且对任意奇素数$q \neq p$，均有

$$\left(\frac{E(p)}{E(q)}\right)=\prod_{i=0}^{s}\left(\frac{k^{\lambda_{i+1}}}{E(r_i)}\right),$$

这里s，λ_i和r_i由下列诸式定义：

$$\begin{cases} p=2l_1r_0+\varepsilon_1r_1, & 0<r_1<r_0=q,\\ r_0=2l_2r_1+\varepsilon_2r_2, & 0<r_2<r_1,\\ \cdots & \\ r_{s-1}=2l_{s+1}r_s+\varepsilon_{s+1}r_{s+1}, & 0<r_{s+1}<r_s,\\ r_s=l_{s+2}r_{s+1}, & r_{s+1}=1, \end{cases} \tag{12}$$

其中$\varepsilon_i=\pm 1$ $(i=1,\cdots,s+1)$，$r_i(i=1,\cdots,s)$均为奇数，而

$$\lambda_i=\begin{cases} l_i, & \text{当}\varepsilon_i=1\text{时}\\ l_i-1, & \text{当}\varepsilon_i=-1\text{时} \end{cases} \quad (i=1,2,\cdots,s+1)。$$

利用这个结果，可以处理方程

$$\frac{\alpha^{pm}+\beta^{pm}}{\alpha^m+\beta^m}=py^2。 \tag{13}$$

例如在$p\equiv 7 \pmod 8$时，取$q=p-2$，则有

$$\begin{aligned} &p=2q-(q-2),\\ &q=2(q-2)-(q-4),\\ &\cdots\\ &q-2(s-1)=2(q-2s)-(q-2(s+1)), \end{aligned}$$

其中$q-2(s+1)=1$。与(12)式比较知$\varepsilon_i=-1$，$l_i=1$ $(i=1,\cdots,s+1)$，故$\lambda_i=0(i=1,\cdots,s+1)$，于是$\left(\frac{E(p)}{E(q)}\right)=1$。

对(13)式取模$E(q)$得

$$\left(\frac{E(p)}{E(q)}\right)=\left(\frac{p}{E(q)}\right)=\left(\frac{E(q)}{p}\right)=1, \tag{14}$$

易知$E(q)\equiv q(-k^m)^{\frac{q-1}{2}}(\bmod p)$，由$q=p-2, p\equiv 7(\bmod 8)$知，(14)式给出

$$1=\left(\frac{E(q)}{p}\right)=\left(\frac{q}{p}\right)=\left(\frac{-2}{p}\right)=-1,$$

这是矛盾的。

定理5可以应用到较为一般的Lucas 序列上。例如对于Lucas序列

$$v_0=2,\ v_1=2a,\ v_{n+2}=2av_{n+1}-kv_n, \tag{15}$$

令$a^2-k=Db^2$，D无平方因子，则在定理5的条件下，(15)中除$\frac{v_0}{2}=1$ 外，$\frac{v_n}{2}$不是平方数。

参 考 文 献

［1］ Stanton, R.G. and Sprott, D. A., Canadian J. Math.,10(1958), 73—77.

［2］ Hall, M.Jr.,Combinatorial Theory,Blaisdell (1967).

［3］ 孙琦，周小明，科学通报，1(1984)，61。

［4］ 曹珍富，自然杂志，6(1985)，476—477。

［5］ 曹珍富，数学研究与评论，3(1987),411—413。

［6］ 曹珍富，东北数学，1(1987)，112—116。

［7］ 曹珍富，自然杂志，9(1986)，720。

［8］ Guy,R.K., Unsolved Problems in Number Theory,Springer—Verlag,New York, 1981, 87.

［9］ 曹珍富，王笃正，科学通报，14(1987)，1043—1046.

［10］ 曹珍富，科学通报，7(1986)，555—556。

[11] 曹珍富，哈尔滨工业大学学报，4(1987)，113—121。
[12] 曹珍富，哈尔滨工业大学学报，3(1986)，112—113。
[13] Perisastri, M., Math. Stud., 37(1969), 211—212.
[14] 曹珍富，扬州师院学报(自然科学版)，1(1986)，17—20。
[15] Toyoizumi, M., Math. Stud., 46(1978) , 113—115(1982).
[16] 曹珍富，科学通报，14(1985)，1116—1117。
[17] 曹珍富，哈尔滨工业大学学报，3 (1986) ，7—11。
[18] 曹珍富，王笃正，扬州师院学报（自然科学版）1987,No.4.
[19] Nagell, T., Arkiv för Mat.,3(1958),569—581.
[20] Makowski, A., Nordisk Mat. Tidskr, 7(1959), 96.
[21] Hadano, T.,Math. J. Okayama Univ., 19(1976), 25—29.
[22] Uchiyama, S., Math.J. Okayama Univ., 19(1976), 30—31.
[23] 杨晓卓,四川大学学报(自然科学版)，4(1985)，151—158.
[24] 曹珍富，科学通报，22(1986)，1688—1690。
[25] Jeśmanowicz, L.,Roczn. Polsk. towarz.

mat., Ser.2, 1(1956), 196—202。

[26] Sierpiński, W., Roczn. Polsk. towarz. mat., Ser.2, 1(1956), 194—195.

[27] 柯召，四川大学学报（自然科学版），1(1958), 73—80。

[28] 柯召，四川大学学报（自然科学版），2(1958), 81—90。

[29] 饶德铭，四川大学学报(自然科学版),1(1960), 79—80。

[30] 柯召，孙琦，四川大学学报（自然科学版）, 3(1964), 1—6。

[31] 柯召，四川大学学报（自然科学版），4(1964), 11—24。

[32] Dem'janenko, V.A., Izv. Vysš. Učebn. Zaved. Matematika,48(1965),No.5,52—56.

[33] 陆文端，四川大学学报(自然科学报),2(1959), 39—41。

[34] Józefiak,T.,Prace Mat.,5(1961),119—123.

[35] 柯召，四川大学学报（自然科学版），3(1959), 24—34。

[36] 陈景润，四川大学学报（自然学科学版）, 2(1962), 19—25。

[37] 曹珍富，数学通讯，6(1982), 35—36。

[38] 曹珍富，哈尔滨工业大学科研报告,253(1982), 11—12。

[39] Brauer, R.,Amer. J. Math., 64(1942), 401—440.

[40] Alex, L.J., Pacific J. Math.,104(1983), 257—262.

[41] Alex, L.J., Math. Comp., 44(1985),267—278.

[42] Alex, L.J., Mrch. Math., 45(1985), 538—545.

[43] Alex, L.J. and Foster, L.L., Rocky Mt. J. Math., 13(1983), 321—331.

[44] 曹珍富,黎进香,哈尔滨工业大学学报,4(1986), 125.

[45] Alex, L.J., Comm. in Algebra, 4(1976), 77—100.

[46] Brenner, J.L. and Foster, L.L., Pacific J. Math.,101(1982), 263—301.

[47] Kutsuna, M., Mem. Gifu Teach. Coll., 21(1986), 25—28.

[48] Johnson, W.,Amer. Math. Monthly, 94(1987), 59—62.

[49] Apéry, R.,C.R. Acad. Sci. Paris Sér.A, 251(1960), 1263—1264.

[50] Browkin, J.and Schinzel, A.,Bull. Acad. Polon. Sci.,Sér. Sci. Math. Astronom. Phys. 8(1960), 311—318.

[51] Schinzel, A.,Acta Arith.,13(1967), 177—236。

[52] Beukers, F., Acta Arith.,38(1981), 389—410.

[53] Apéry, R., C.R. Acad. Sci.Paris, Sér. A, 251(1960), 1451—1452.

[54] Alter, R.and Kubota, K.K., Pacific J. Math., 46(1973), 11—16.

[55] Kutsuna,M.,Mem. Gifu Nat. Coll. Tech., 20(1985), 57—60.

[56] Beukers, F.,The generalised Ramanujan—Nagell equation, Doct. thesis, Rijks,1979.

[57] Kutsuna,M.,Mem. Gifu Nat. Coll. Tech., 18(1983), 65—68.

[58] 乐茂华，科学通报，5(1984)，268—271.

[59] Beukers,F.,Acta Arith.,39(1981),113—123.

[60] Toyoizumi, M., Comment. Math. Univ. St. Pauli, 27(1979), 105—111.

[61] Toyoizumi, M., Acta Arith., 42(1983), 303—309.

[62] Yamabe, M., Reports Fac. Sci. Tech. Meijyo Univ., 21(1981), 205—207.

[63] Yamabe, M., ibid, 20(1979), 186—189; 24(1984), 1—5.

[64] Kutsuna, M., Mem. Gifu Nat. Coll. Tech., 20(1985), 61—62.

[65] 孙琦，曹珍富，关于方程 $x^2+D^m=p^n$ 和 $x^2+2^m=y^n$，四川大学学报（自然科学版），2(1988)，164—169。

[66] 柯召，J.Chinese Math. Soc., 2(1940), 205—207.

[67] Schinzel, A., 四川大学学报（自然科学版），1(1958), 81—83。
[68] 阎发湘，科学通报，12(1980), 529—532。
[69] Dem'janenko, V.A., Izv. Vysš. Učebn. Zaved. Matematika, 159(1975), No.8, 39—45.
[70] Mills, W.H., Report Inst. Theory of Numbers, Boulder, Colo. 1959, 253—268.
[71] Uchiyama, S., Trudy Mat. Inst. Steklov., 163(1984), 237—243.
[72] 阎发湘，辽宁大学学报(自然科学版), 1(1980), 27—28。
[73] 姚兆栋，数学杂志，1(1983), 9—12。
[74] 瞿维建，浙江师范大学学报（自然科学版），1(1987), 59—64。
[75] 柯召，四川大学学报（自然科学版），1(1957), 30—40。
[76] 柯召，陆文端，四川大学学报（自然科学版），2(1957), 189—195。
[77] Calderbank, R., J. London Math. Soc., (2)26(1982), 365—384.
[78] Bremner, A. et al., J. Number Theory, 16(1983), 212—234.
[79] Bremner, A. and Morton, P., Math. Comp., 39(1982), 235—238.
[80] Tzanakis, N. and Wolfskill, J., J. Number Theory, 23(1986), 219—239.
[81] Tzanakis, N. and Wolfskill, J., J. Number

Theory, 26(1987), 96—116.

[82] Johnson, W., Amer. Math. Monthly, 94(1987), 59—62.

[83] 柯召，孙琦，四川大学学报（自然科学版），1(1975), 57—61。

[84] 曹珍富，哈尔滨工业大学学报,4(1981),53—58。

[85] 孙琦，四川大学学报（自然科学版），3(1986), 16—19。

[86] 曹珍富，一类不定方程对Lucas序列的应用（已投稿）。

[87] 柯召、孙琦，四川大学学报（自然科学版）。2(1964), 5—9。

第十章　单位分数问题

所谓单位分数是指分子为1而分母为任意正整数的分数。关于单位分数，有一个古老的问题：把一个正有理数（包括正整数）表成单位分数的和，即对给定的正整数m,n，解丢番图方程

$$\frac{m}{n}=\frac{1}{x_1}+\cdots+\frac{1}{x_k}。$$

与这个方程相关的问题，一直吸引着人们的广泛兴趣，其中有许多问题至今尚未解决。本章的目的，就是讨论这方面人们感兴趣的问题，并详细介绍对它们研究的成果和方法。

§1　方程 $\frac{m}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$

设m,n是正整数，我们来研究丢番图方程

$$\frac{m}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \qquad (1)$$

的正整数解。1950年，Erdös猜想：对每一个正整数$n>1$，方程

$$\frac{4}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \qquad (2)$$

均有正整数解x,y,z。后来，Straus作了更强地猜想：设$n>2$，则方程(2)有两两不等的正整数解。并且他对$2<n<$

5000证明了猜想是对的（见[1]）。1964年，柯召、孙琦和张先觉[2]证明了Straus 猜想与Erdös猜想是等价的，并证明了$n<4\times10^5$时Erdös—Straus 猜想成立。1965年，Yamamoto[3]把n的界推到$n<10^7$。1978年，n的界又被Franceschine[4]推到10^8。这些结果的证明都使用了一些基本事实，通过构造n的一些同余条件获得方程(2)的解。这些基本事实如下：

1）如果$n>1$使得方程(2)有解(x_1,y_1,z_1)，则n的任何倍数mn也使得方程(2)有解，且解为(mx_1,my_1,mz_1)。

2）如果有正整数a,b,c,d满足

$$a+bn+cn=4abcd, \qquad (3)$$

或

$$na+b+c=4abcd, \qquad (4)$$

则方程(2)有解，且解分别为$(x,y,z)=(bcdn,acd,abd)$和$(bcd,nabd,nacd)$。

从(4)式，取$a=2$，$b=1,c=1$,则$n=4d-1$；取$a=1,b=1,c=1$,则$n=4d-2$。故在$n\equiv2,3\pmod 4$时方程(2)有正整数解。

当$n\equiv0\pmod 4$时，(2)显然有正整数解$x=y=z=\frac{3n}{4}$。这样，我们只要考虑$n\equiv1\pmod 4$就行了。

又在(4)中，取$a=1,b=1,c=2$,则$n=8d-3$。故在$n\equiv5\pmod 8$时方程(2)有解。现设$n\equiv1\pmod 8$。

利用这种方法，可以十分容易地给出$n\not\equiv1\pmod 3$，$n\not\equiv1,2,4\pmod 7$，$n\not\equiv1,4\pmod 5$时方程(2)均有正整数解。由此可推出，除开

$$n\equiv1,11^2,13^2,17^2,19^2,23^2\pmod{840} \qquad (5)$$

（由1）不妨设n为素数）外，Erdös—Straus猜想成立。

由于满足(5)的最小素数是1009，故在$n<1009$时Erdös—Straus猜想成立。如果由(3)和(4)，在840中再添上一些因子，则可把n的上界继续放大。

现在设$n=p>3$，p是一个素数，则不妨设$p\nmid(x,y,z)$，于是$p|x, p\nmid yz$或$p|y, p|z$且$p\nmid x$。这样方程(2)化为如下的两个方程

$$\frac{4}{p}=\frac{1}{px}+\frac{1}{y}+\frac{1}{z}, p\nmid yz, \tag{6}$$

$$\frac{4}{p}=\frac{1}{x}+\frac{1}{py}+\frac{1}{pz}, p\nmid x。 \tag{7}$$

对此，Rosati[5]证明了

定理1 方程(6)有解当且仅当存在正整数a,b,c,d使得

$$a+bp+cp=4abcd, (a,b)=(b,c)=(c,a)=1, p\nmid abcd, \tag{8}$$

且(8)成立时$(x,y,z)=(bcd,acd,abd)$。

定理2 方程(7)有解当且仅当存在正整数a,b,c,d使得

$$pa+b+c=4abcd, (a,b)=(b,c)=(c,d)=1, p\nmid bcd, \tag{9}$$

且(9)成立时$(x,y,z)=(bcd,abd,acd)$。

我们这里仅给出定理1的证明（定理2的证明完全类似）。设$(y,z)=\delta$, $y=\delta b, z=\delta c$，这里$p\nmid bc\delta$，由(6)式得

$$\delta bc+p(b+c)x=4\delta bcx。 \tag{10}$$

因为$(b+c,bc)=1$，故(10)式给出$bc|x$，设$x=bcd$，则(10)式两端除去bc得

$$\delta+p(b+c)d=4\delta dbc。$$

由此知$d|\delta$，令$\delta=da$，则

$$a+p(b+c)=4abcd。$$

这就证明了定理1。

Sierpiński还作了一个类似地猜想：对每一个$n>1$，方程

$$\frac{5}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \tag{11}$$

均有正整数解。利用前面类似的方法，Palamà[6,7]证明了$n<922321$时Sierpiński猜想成立。Stewart[8]改进n的界到$n\leqslant 1057438801$且$n\not\equiv 1(\bmod\ 278460)$。

在方程(11)中，如果$n=121$，则(11)有解$(x,y,z)=(25,759,208725)$。1984年，刘元章[9]给出了方程

$$\frac{5}{121}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z} \tag{12}$$

的全部正整数解。不妨设$0<x<y<z$，则(12)的全部正整数解由下表给出：

x	y	z	x	y	z	x	y	z
25	759	208725	26	352	50336	33	93	3751
25	770	42350	26	363	9438	33	99	1089
25	825	9075	27	234	84942	33	121	363
25	1089	2475	27	242	6534	34	84	172788
25	1100	2420	27	297	1089	44	54	13068
26	350	272175	30	132	2420	44	55	2420
26	351	84942	33	91	33033	45	55	1089

这也回答了Blericher的一个问题。

对于一般的方程(1)，设$Em(N)$表示不大于N且使方程(1)无正整数解的n的个数，则有如下的Vaughan[10]定理：

定理3 $E_m(N)\ll N\cdot\exp[-c(\log N)^{2/3}]$，这里$c$是仅取决于$m$的常数。

对于一般的方程

$$\frac{m}{n}=\frac{1}{x_1}+\cdots+\frac{1}{x_k},\tag{13}$$

以$E_{m,k}(N)$表示不大于N且使方程(13)无正整数解的n的个数，Viola[11]在1973年年证明了

$$E_{m,k}(N)\ll N\cdot\exp[-c(\log N)^{1-\frac{1}{k-1}}]。$$

1986年，单墫[12]改进了Viola的结果，证明了

$$E_{m,k}(N)\ll N\cdot\exp[-c(\log N)^{1-\frac{1}{k}}],$$

这里c仅取决于m与k。从而把Vaughan的结果推广到一般的情形。

§2 Mordell的一个问题

Mordell[13]曾经提出一个单位分数的问题：

方程

$$\frac{1}{w}+\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{wxyz}=0\tag{1}$$

的解如何？曹珍富[14]首先讨论了方程(1)的解。显然x,y,z,w必至少有一个为正且至少有一个为负，不妨设$x>0$，$w<0$。对y,z有三种情形：同正、同负或一正一负。于是方程(1)化为如下三个求正整数解的方程：

$$\frac{1}{x}=\frac{1}{y}+\frac{1}{z}+\frac{1}{w}+\frac{1}{xyzw},\tag{2}$$

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{xyzw}=\frac{1}{z}+\frac{1}{w},\tag{3}$$

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{1}{w}+\frac{1}{xyzw}。\tag{4}$$

显然，(2)～(4)都给出x,y,z,w两两互素。对方程(2)，不妨设$y<z<w$，则有

定理1 方程(2)的全部正整数解可表为

$$\begin{cases} x=n, \\ y=n+k, \\ z=n+\dfrac{n^2+t}{k}, \\ w=\dfrac{1}{t}\left[n(n+k)\left(n+\dfrac{n^2+t}{k}\right)+1\right], \end{cases} \tag{5}$$

这里n,k,t为正整数，且满足

1) $n^2+t\equiv 0 \pmod{k}$；

2) $n(n+k)\left(n+\dfrac{n^2+t}{k}\right)+1\equiv 0 \pmod{t}$；

3) $(n,k)=(k,t)=(n,t)=1$。

证 由(5)代入(2)验证知，(5)确为(2)的解。现设$x=n$，则显然$y>n$，这里n为正整数，令$y=n+k$，k为正整数，由(2)得

$$\frac{k}{n(n+k)}=\frac{1}{z}+\frac{1}{w}+\frac{1}{k(n+k)zw}。 \tag{6}$$

令$m=\dfrac{n(n+k)}{k}$，则$z>m$，可设$z=m+s$，$s>0$。于是(6)给出

$$\frac{s}{m(m+s)}=\frac{1}{w}+\frac{1}{km(m+s)w},$$

由此知

$$skw=km(m+s)+1。 \tag{7}$$

由于$z=m+s=n+\dfrac{n^2}{k}+s$为正整数，设$(n,k)=d$，则必有

$s=\dfrac{dt}{k}$，且$k|n^2+dt$。由(7)得出

$$dtw=n(n+k)\left(n+\frac{n^2+dt}{k}\right)+1,$$

由于$d|n$，故上式给出$d|1$，所以$d=1$。上式成为

$$w=\frac{1}{t}\left[n(n+k)\left(n+\frac{n^2+t}{k}\right)+1\right]。$$

容易知道1)～3)的条件均成立。证毕。

由(5)可以给出方程(2)的许多含参数的解，例如在定理1中分别取$k=t=1$，和$t=1,k=2m^2+\varepsilon 2m+1,n=2m^2+k\lambda$即得

Ⅰ. $x=n,\ y=n+1,z=n(n+1)+1,\ w=n(n+1)[n(n+1)+1]+1$；

Ⅱ. $x=2m^2+(2m^2+\varepsilon 2m+1)\lambda,\ y=2m^2+(2m^2+\varepsilon 2m+1)(\lambda+1),z=4m^2-\varepsilon 2m+1+4m^2\lambda+(2m^2+\varepsilon 2m+1)\lambda(\lambda+1),w=xyz+1$，这里$\varepsilon=\pm 1,m,\lambda$是正整数。

在$t=1$时，由于(5)中$w=xyz+1$，故方程(2)简化为

$$\frac{1}{x}=\frac{1}{y}+\frac{1}{z}+\frac{1}{xyz} \qquad (8)$$

且有

$$x=n,y=n+k,z=n+\frac{n^2+1}{k},$$

这里$n^2+1\equiv 0(\bmod\ k)$。我们对小于100的素数k，求出了满足$n^2+1\equiv 0(\bmod\ k)$的n，k，从而得出方程(8)有如下的解：

x	y	z
$2m+1$	$2m+3$	$2(m+1)^2$

x	y	z
$5m+2$	$5m+7$	$5m^2+9m+3$
$5m+3$	$5m+8$	$5m^2+11m+5$
$13m+5$	$13m+18$	$13m^2+23m+7$
$13m-5$	$13m+8$	$13m^2+3m-3$
$17m+4$	$17m+21$	$17m^2+25m+5$
$17m-4$	$17m+13$	$17m^2+9m-3$
$29m+12$	$29m+41$	$29m^2+53m+17$
$29m-12$	$29m+17$	$29m^2+5m-7$
$37m+6$	$37m+43$	$37m^2+49m+7$
$37m-6$	$37m+31$	$37m^2+25m-5$
$41m+9$	$41m+50$	$41m^2+59m+11$
$41m-9$	$41m+32$	$41m^2+23m-7$
$53m+23$	$53m+76$	$53m^2+99m+33$
$53m-23$	$53m+30$	$53m^2+7m-13$
$61m+11$	$61m+72$	$61m^2+83m+13$
$61m-11$	$61m+50$	$61m^2+39m-9$
$73m+27$	$73m+100$	$73m^2+127m+37$
$73m-27$	$73m+46$	$73m^2+19m-17$
$89m+34$	$89m+123$	$89m^2+157m+47$
$89m-34$	$89m+55$	$89m^2+21m-21$
$97m+22$	$97m+119$	$97m^2+141m+27$
$97m-22$	$97m+75$	$97m^2+53m-17$

设x_1,y_1,z_1是(8)的任一组正整数解，易知$(x_1,y_1,z_1,x_1y_1z_1+1)$是方程(2)的一组正整数解。因此在上表加一行$w=xyz+1$，则上表也给出了方程(2)的解。一般地，设$(x_1,\cdots,x_{s-1})$满足方程

$$\frac{1}{x_1}=\frac{1}{x_2}+\cdots+\frac{1}{x_{s-1}}+\frac{1}{x_1\cdots x_{s-1}},$$

则$(x_1,\cdots,x_s)$，这里$x_s=x_1\cdots x_{s-1}+1$，满足方程

$$\frac{1}{x_1}=\frac{1}{x_2}+\cdots+\frac{1}{x_s}+\frac{1}{x_1\cdots x_s},\qquad (9)$$

故由我们关于方程(2)的解（在$t=1$时由(8)的解构造出来）可以构造出方程(9)的解。

如果我们把方程(2)的解(5)分成几类：$t=k=1$的解称为平凡解（见Ⅰ）；$t=1,k>1$的解称为A类解；$t>1,k=1$称为B类解；$t>1,k>1$称为AB类解。则前面我们给出了方程(2)的平凡解和若干A类解。在第二章的§8中，我们给出了AB类解的构造方法。

对于B类解的构造也是容易的。例如在$k=1$时，由(5)知$x=n,y=n+1$，故方程(2)化为

$$\frac{1}{n(n+1)}=\frac{1}{z}+\frac{1}{w}+\frac{1}{n(n+1)zw}。$$

这具备了方程(8)的形式，故可用构造A类解的方法来构造方程(2)的B类解。例如取$n=5m+1,t=5$，则(5)给出方程(2)有解

$$x=5m+1,y=5m+2,z=25m^2+15m+7,$$
$$w=125m^4+150m^3+90m^2+17m+3。$$

与对方程(2)的讨论完全类似，可以给出方程(3)、(4)的解及构造方法。

定理2 方程(3)的全部正整数解（不妨设$x>w$）可表为

$$\begin{cases}x=n+k,\\ y=n+\dfrac{n^2-t}{k},\\ z=\dfrac{1}{t}\left[n^2\left(2n+k+\dfrac{n^2-t}{k}\right)-1\right]-n,\\ w=n,\end{cases}$$

这里n,k,t均是正整数，且满足

1) $n^2-t\equiv 0 \pmod{k}$；

2) $n^2\left(2n+k+\frac{n^2-t}{k}\right)-1\equiv 0 \pmod{t}$；

3) $(n,k)=(k,t)=(n,t)=1$。

定理3 方程(4)的全部正整数解（不妨设$x>w$）可表为

$$\begin{cases} x=n+k, \\ y=n+\frac{n^2+t}{k}, \\ z=n+\frac{1}{t}\left[n^2(2n+k+\frac{n^2+t}{k})-1\right], \\ w=n, \end{cases}$$

这里n,k,t是正整数，且满足

1) $n^2+t\equiv 0 \pmod{k}$；

2) $n^2\left(2n+k+\frac{n^2+t}{k}\right)-1\equiv 0 \pmod{k}$；

3) $(n,k)=(k,t)=(t,n)=1$。

§3 方程 $\sum_{i=1}^{s}\frac{1}{x_i}+\frac{1}{x_1\cdots x_s}=1$

在有关单位分数的问题中，最引人注目的问题要数单位分数表1的问题。设有方程

$$\frac{1}{x_1}+\cdots+\frac{1}{x_k}=1,0<x_1<\cdots<x_k, \tag{1}$$

根据我们在§2中的讨论，方程(1)对任意给定的k都有解$x_1=2,x_{i+1}=x_1\cdots x_i+1(i=4,\cdots,k-2),x_k=x_1\cdots x_{k-1}$。Erdös[15]问：在方程(1)的解中$\max x_k=?$1987年，冯克勤、魏

权龄和刘木兰[16]证明了$\max x_k = x_1 \cdots x_{k-1}$，这里$x_1 = 2$，$x_{i+1} = x_1 \cdots x_i + 1 (i \geqslant 1)$。这说明方程(1)的解中使$x_k$最大的那组解是方程

$$\sum_{i=1}^{s} \frac{1}{x_i} + \frac{1}{x_1 \cdots x_s} = 1,\ 1 < x_1 < \cdots < x_s \qquad (2)$$

在$s = k-1$时的一组解。但是他们的方法对求解方程(2)没有丝毫帮助。由于方程(2)在许多其他问题中的重要应用（参阅§4，§5），所以本节我们专门来讨论方程(2)的解。

1964年，柯召和孙琦[17]首先研究了方程(2)的解，在$s \leqslant 6$时证明了方程(2)仅有如下的解：

s	x_1	x_2	x_3	x_4	x_5	x_6
1	2					
2	2	3				
3	2	3	7			
4	2	3	7	43		
5	2	3	11	23	31	
	2	3	7	43	1807	
	2	3	7	47	953	
6	2	3	11	23	31	47059
	2	3	7	43	1823	193667
	2	3	7	43	1807	32633443
	2	3	7	47	395	779731
	2	3	7	47	403	19403
	2	3	7	47	415	8111
	2	3	7	47	583	1223
	2	3	7	55	179	24323

以$\Omega(s)$表示方程(2)的解的个数，则上表给出$\Omega(1) = \Omega(2) = \Omega(3) = \Omega(4) = 1$，$\Omega(5) = 3$，$\Omega(6) = 8$。他们还

证明了

定理1 若$x_1^{(0)}$, …, $x_{s-1}^{(0)}$满足 $\sum_{i=1}^{s-1}\frac{1}{x_i^{(0)}}+\frac{1}{x_1^{(0)}\cdots x_{s-1}^{(0)}}=1$，且$(x_1^{(0)}\cdots x_{s-1}^{(0)})^2+1$是合数，则有$\Omega(s)<\Omega(s+1)$。

证 由于方程(2)的$\Omega(s)$个解$(x_1^{(j)}, \cdots, x_s^{(j)})(j=1, \cdots, \Omega(s))$可以得出方程

$$\sum_{i=1}^{s+1}\frac{1}{x_i}+\frac{1}{x_1\cdots x_{s+1}}=1, 1<x_1<\cdots<x_{s-1} \qquad (3)$$

的$\Omega(s)$个解$(x_1^{(j)},\cdots,x_s^{(j)}, x_{s+1}^{(j)})$，这里$x_{s+1}^{(j)}=x_1^{(j)}\cdots x_s^{(j)}+1$，故$\Omega(s)\leqslant\Omega(s+1)$。现在证明在$(x_1^{(0)}\cdots x_{s-1}^{(0)})^2+1$为合数时，方程(3)至少有一组不是用方程(2)的解通过$x_{s+1}^{(j)}=x_1^{(j)}\cdots x_s^{(j)}+1$得到。为此，在(3)中令$x_i=x_i^{(0)}(i=1, \cdots, s-1)$，得出

$$\frac{1}{x_s}+\frac{1}{x_{s+1}}+\frac{1}{nx_sx_{s+1}}=\frac{1}{n},$$

这里$n=x_1^{(0)}\cdots x_{s-1}^{(0)}$。于是

$$x_s=n+k, \quad x_{s+1}=n+\frac{n^2+1}{k},$$

因此在n^2+1为合数时，设$n^2+1=m_1m_2$，$1<m_1<m_2$，于是可取$k=m_1$，得到$x_s=n+m_1$，$x_{s+1}=n+m_2$，这就证明$\Omega(s)<\Omega(s+1)$。证毕。

1978年，孙琦[18]证明了

定理2 设$s\geqslant4$，则$\Omega(s)<\Omega(s+1)$。

显然，定理2的证明，只需找到一组$x_1^{(0)}$, …, $x_{s-1}^{(0)}$，满足$\sum_{i=1}^{s-1}\frac{1}{x_i^{(0)}}+\frac{1}{x_1^{(0)}\cdots x_{s-1}^{(0)}}=1$和$(x_1^{(0)}\cdots x_{s-1}^{(0)})^2+1$为合数。

因为(2，3，11，23，31，47059)是方程(2)在$s=6$时的一组解，设$\eta_0=2\cdot3\cdot11\cdot23\cdot31\cdot47059$，

$\eta_1=\eta_0+1, \eta_2=\eta_0\eta_1+1, \cdots, \eta_{s-1}=\eta_0\cdots\eta_{s-2}+1 (s\geqslant 3)$，则$x_1^{(0)}=2, \cdots, x_6^{(0)}=47059, x_7^{(0)}=\eta_1, \cdots, x_{s-1}^{(0)}=\eta_{s-7}$满足$\sum_{i=1}^{s-1}\frac{1}{x_i^{(0)}}+\frac{1}{x_1^{(0)}\cdots x_{s-1}^{(0)}}=1$，且在$2\nmid s\geqslant 7$时$(x_1^{(0)}\cdots x_{s-1}^{(0)})^2+1=(\eta_0\eta_1\cdots\eta_{s-7})^2+1\equiv 0 \pmod 5$。故在$2\nmid s\geqslant 7$时定理2成立。

从方程(2)在$s=3$时的解(2，3，7)，与前同样道理可知，在$2|s\geqslant 4$时$\Omega(s)<\Omega(s+1)$。

再由$\Omega(4)=1$，$\Omega(5)=3$，$\Omega(6)=8$便知定理2成立。

同在1978年，Janák和Skula[19]利用计算机也给出了方程(2)在$s\leqslant 6$时的全部解，且在$s=7$时他们得到了方程(2)的18组解，即$\Omega(7)\geqslant 18$。

1984年，孙琦和曹珍富[20]改进了定理1，得到了较为精密的

定理3 若$x_1^{(j)}, \cdots, x_{s-1}^{(j)} (j=1, \cdots, \Omega(s-1))$是方程$\sum_{i=1}^{s-1}\frac{1}{x_i}+\frac{1}{x_1\cdots x_{s-1}}=1$的$\Omega(s-1)$个解，记$k_j(s)=(x_1^{(j)}\cdots x_{s-1}^{(j)})^2+1 (j=1, \cdots, \Omega(s-1))$，则有

$$\Omega(s+1)\geqslant\Omega(s)+\sum_{j=1}^{\Omega(s-1)}\left(\frac{d(k_j(s))}{2}-1\right),$$

这里$d(k_j(s))$表$k_j(s)$的不同正因子的个数$(j=1, \cdots, \Omega(s-1))$。

同时构造性地证明了

定理4 设$s\geqslant 10$，则$\Omega(s+1)\geqslant\Omega(s)+3$，且在$2|s\geqslant 10$时$\Omega(s+1)\geqslant\Omega(s)+5$。

1986年，孙琦和曹珍富[21]进一步地证明了

定理5 设$s \geqslant 10$，则$\Omega(s+1) \geqslant \Omega(s)+5$，且在$2 \nmid s \geqslant 11$时$\Omega(s+1) \geqslant \Omega(s)+7$。

以上结果都是基于方程(2)在$s=6$时的全部解以及$s=7$时的18组解使用§2的构造方法获得的。可以看出，进一步给出$s=7$（或更大）的全部解，对改进$\Omega(s)$是有帮助的。

1987年，曹珍富、刘锐和张良瑞[22]利用计算机给出了方程(2)在$s=7$时的全部解，共26组（见表1）。

表1

序	x_1	x_2	x_3	x_4	x_5	x_6	x_7	$y_7=(x_1 \cdots x_6+1)/x_7$
1	2	3	7	43	1807	3263443	10650056950807	1
2	2	3	7	43	1807	3263447	2130014000915	5
3	2	3	7	43	1807	3263591	71480133827	149
4	2	3	7	43	1807	3264187	14298637519	745
5	2	3	7	43	1823	193667	637617223447	1
6*	2	3	7	43	3559	3667	33316127	697
7	2	3	7	47	395	779731	607979652631	1
8	2	3	7	47	395	779831	6020372531	101
9	2	3	7	47	403	19403	15435513367	1
10	2	3	7	47	415	8111	6644612311	1
11	2	3	7	47	583	1223	1407479767	1
12	2	3	7	55	179	24323	10057317271	1
13*	2	3	7	67	187	283	334651	445
14*	2	3	11	17	101	149	3109	5431
15	2	3	11	23	31	47059	2214502423	1
16	2	3	11	23	31	47063	442938131	5
17	2	3	11	23	31	47095	59897203	37
18	2	3	11	23	31	47131	30382063	73
19	2	3	11	23	31	47243	12017037	185
20	2	3	11	23	31	47423	6114059	365

续表

序	x_1	x_2	x_3	x_4	x_5	x_6	x_7	$y_7=(x_1\cdots x_6+1)/x_7$
21*	2	3	11	23	31	49759	866923	2701
22*	2	3	11	23	31	60563	211031	13505
23	2	3	11	31	35	67	369067	13
24*	2	3	7	43	3263	4051	2558951	1227
[注] 25*	2	3	11	25	29	1097	2753	19067
26*	2	3	13	25	29	67	2981	1271

注. [22]中漏了三组解

利用我们新发现的解，把$\Omega(s)$改进到：设$s\geqslant 11$，则$\Omega(s+1)\geqslant\Omega(s)+8$，且在$2\nmid s\geqslant 11$时$\Omega(s+1)\geqslant\Omega(s)+9$。

最近，曹珍富[23]利用$s=7$时的26组解，大大地改进了前述的结果，构造性地证明了

定理6 设$s\geqslant 11$，则$\Omega(s+1)\geqslant\Omega(s)+17$，且在$2\nmid s\geqslant 11$时$\Omega(s+1)\geqslant\Omega(s)+23$。

这个定理的证明思路是，针对表1中的每一组x_1，…，x_7，求出$(x_1\cdots x_7)^2+1$的所有不超过100的素因子。然后，可以验证：在方程(2)当s换为$s-1$时有17组x_1，…，x_{s-1}使得

当$2\mid s\geqslant 12$时$(x_1\cdots x_{s-1})^2+1\equiv 0\pmod 5$；

有23组x_1，…，x_{s-1}使得

当$2\nmid s\geqslant 11$时$(x_1\cdots x_{s-1})^2+1\equiv 0\pmod 5$。

故由定理3知：

当$2\mid s\geqslant 12$时$\Omega(s+1)\geqslant\Omega(s)+17$，

当$2\nmid s\geqslant 11$时$\Omega(s+1)\geqslant\Omega(s)+23$。

表2和表3分别给出17组（当$2\mid s\geqslant 12$时）和23组（当$2\nmid s$

$\geqslant 11$时）x_1，…，x_{s-1}使$(x_1\cdots x_{s-1})^2+1\equiv 0 \pmod 5$的详细情况。

表2

序	表1中的序	$x_1, \cdots, x_{s-1}$ ($s\geqslant 12$)	
1	1		
2	5	$x_1,\cdots,x_7$（由对照表1中的每一个序分别给出）：	
3	9	$x_8=x_1\cdots x_7+1, x_9=x_1\cdots x_7x_8+1,$	
4	11	$x_{10}=x_1\cdots x_9+1,\cdots,x_{s-1}=x_1\cdots x_{s-2}+1$	
5	14		
6	9	$x_1,\cdots,x_7$（见表1）：	$f=17\cdot 53$
7	9	$x_8=x_1\cdots x_7+f,$	$f=37\cdot 53$
8	9	$x_9=x_1\cdots x_7+\frac{(x_1\cdots x_7)^2+1}{f}$	$f=5\cdot 17\cdot 37$
9	14	$\cdots,$	$f=5$
10	24	$x_{s-1}=x_1\cdots x_{s-2}+1$	$f=5$
11	6	$x_1,\cdots,x_7$（见表1）：$x_8=x_1\cdots x_7+1,$	$f=5$
12	6	$x_9=x_1\cdots x_8+f,$	$f=5\cdot 29$
13	11	$x_{10}=x_1\cdots x_8+\frac{(x_1\cdots x_8)^2+1}{f},\cdots,$	$f=17$
14	15	$x_{s-1}=x_1\cdots x_{s-2}+1$	$f=17$
15	9	$x_1,\cdots,x_6$（见表1）*：$x_7=x_1\cdots x_6+f,$	$f=97$
16	15	$x_8=x_1\cdots x_6+\frac{(x_1\cdots x_6)^2+1}{f},\cdots,$	$f=51$
17	11	$x_{s-1}=x_1\cdots x_{s-2}+1$	$f=41$

*这时取表1中对应$y_7=1$的那些行删除x_7所在的列剩下的$x_1,\cdots,x_6$。

表3

序	表1中的序	$x_1, \cdots, x_{s-1}$ $(s \geqslant 11)$	
1	4		
2	6	$x_1, \cdots, x_7$（见表1）：	
3	15	$x_8 = x_1 \cdots x_7 + 1$	
4	19	$x_9 = x_1 \cdots x_8 + 1$	
5	20	$x_{10} = x_1 \cdots x_9 + 1, \cdots,$	
6	21	$x_{s-1} = x_1 \cdots x_{s-2} + 1$	
7	24		
8	6		$f=37$
9	6		$f=13 \cdot 37$
10	9	$x_1, \cdots, x_7$（见表1）：	$f=17$
11	9		$f=37$
12	9	$x_8 = x_1 \cdots x_7 + f,$	$f=5 \cdot 17$
13	9		$f=5 \cdot 37$
14	9	$x_9 = x_1 \cdots x_7 + \frac{(x_1 \cdots x_7)^2 + 1}{f},$	$f=17 \cdot 37 \cdot 53$
15	9	$\cdots,$	$f=5 \cdot 17 \cdot 37 \cdot 53$
16	19	$x_{s-1} = x_1 \cdots x_{s-2} + 1$	$f=29$
17	19		$f=5 \cdot 13$
18	19		$f=5 \cdot 13 \cdot 29$
19	11		$f=5$
20	4	$x_1, \cdots, x_7$（见表1）：$x_8 = x_1 \cdots x_7 + 1,$	$f=5$
21	4	$x_9 = x_1 \cdots x_8 + f,$	$f=61$
22	4	$x_{10} = x_1 \cdots x_8 + \frac{(x_1 \cdots x_8)^2 + 1}{f}$	$f=5 \cdot 61$
23	6	$\cdots, x_{s-1} = x_1 \cdots x_{s-2} + 1$	$f=5^2 \cdot 29$

我们还构造性地给出$\Omega(8) \geqslant 34$，$\Omega(9) \geqslant 67$，$\Omega(10) \geqslant 83$，等等。

由定理6还可推出

推论 当$s\geqslant 11$时$\Omega(s)\geqslant 20s+\Omega(11)-220$。

但是，我们没有定出$\Omega(s)$的渐近公式。我们[24]也不知道是否对任意给定的正整数$x_1>1$，都存在正常数c，使得当$s\geqslant c$时方程(2)均有整数解。对$\Omega(s)$，我们有一个直观地推断：存在某个正常数c,在$\min(s, t)>c$时均有$\Omega(s+t+1)\geqslant\Omega(s+t)+\Omega(s)+s$成立。但没有得到证明。

§4 方程 $\sum_{i=1}^{s}\frac{1}{x_i}-\frac{1}{x_1\cdots x_s}=1$

解丢番图方程

$$\sum_{i=1}^{s}\frac{1}{x_i}-\frac{1}{x_1\cdots x_s}=1,\ 1<x_1<\cdots<x_s,\ s>2 \quad (1)$$

是孙琦和曹珍富[25]提出来的。我们知道，初等数论中的孙子定理有着广泛地应用，例如，利用孙子定理可构造模系数记数法[26, 27]：设$s>1$，m_1，…，m_s是两两互素的正整数（均大于1），$M=m_1\cdots m_s$，$0\leqslant x<M$，则x的模系数记数法是指x对模$m_1,\cdots,m_s$的剩余表示$\{\langle x\rangle_{m_1},\cdots,\langle x\rangle_{m_s}\}$。如果知道$x$的模系数记数法，则用孙子定理可得

$$x=\left\langle\sum_{i=1}^{s}M_i'M_i\langle x\rangle_{m_i}\right\rangle_M,$$

其中$M_i=\frac{M}{m_i}(i=1,\ \cdots,\ s)$，且

$$M_i'M_i\equiv 1(\bmod\ m_i)(i=1,\ \cdots,\ s)。\quad (2)$$

在这个过程中，如何选择m_1，…，m_s使得计算M_i'容易（尤

其在s很大时），是一个实际应用的问题。我们证明了

定理1 如果m_1，…，m_s取方程(1)的一组解，则对模m_1，…，m_s，(2)式中的M'_i可取为$M'_i=1(i=1, \cdots, s)$。

证 如果m_1，…，m_s取方程(1)的一组解，则有

$$\sum_{i=1}^{s}\frac{1}{m_i}-\frac{1}{m_1\cdots m_s}=1,$$

故得$\sum_{i=1}^{s}M_i-1=M$，这就给出$M_i\equiv 1(\bmod m_i)(i=1,\cdots,s)$，因此可取$M'_i=1(i=1, \cdots, s)$。证毕。

现在的问题是，方程(1)是否有解？有多少解？为了便于实际应用，我们给出了在$3\leqslant s\leqslant 6$时方程(1)的全部解（$s=6$时见[28]），见下页表。

我们同时给出，可以通过方程

$$\sum_{i=1}^{s}\frac{1}{x_i}+\frac{1}{x_1\cdots x_s}=1,\quad 1<x_1<\cdots<x_s \tag{3}$$

的解（见§3）来构造方程(1)的解的方法。

定理2 设$x_1^{(j)}$，…，$x_{s-1}^{(j)}(j=1, \cdots, \Omega(s-1))$是方程(3)在$s$换为$s-1$的$\Omega(s-1)$组解，$l_j(s)=(x_1^{(j)}\cdots x_{s-1}^{(j)})^2-1(j=1, \cdots, \Omega(s-1))$，则方程(1)的解的个数$A(s)$满足

$$A(s+1)\geqslant\Omega(s)+\sum_{j=1}^{\Omega(s-1)}\left(\frac{d(l_j(s))}{2}-1\right), \tag{4}$$

这里$d(l_j(s))$表$l_j(s)$不同正因子的个数。

证 在方程

$$\sum_{i=1}^{s+1}\frac{1}{x_i}-\frac{1}{x_1\cdots x_{s+1}}=1 \tag{5}$$

中令$x_i=x_i^{(j)}(i=1, \cdots, s-1)$，则得

s	x_1	x_2	x_3	x_4	x_5	x_6
3	2	3	5			
4	2	3	7	41		
	2	3	11	13		
5	2	3	7	43	1805	
	2	3	7	83	85	
	2	3	7	41	1721	
	2	3	11	17	59	
6	2	3	7	43	1807	3263441
	2	3	7	43	1811	654133
	2	3	7	43	1819	252701
	2	3	7	43	1825	173471
	2	3	7	43	1945	25271
	2	3	7	43	1871	51985
	2	3	7	43	1901	35139
	2	3	7	43	2053	15011
	2	3	7	43	2167	10341
	2	3	7	43	2501	6499
	2	3	7	43	3041	4447
	2	3	7	43	3611	3613
	2	3	7	47	395	779729
	2	3	7	47	481	2203
	2	3	7	53	271	799
	2	3	7	71	103	61429
	2	3	11	23	31	47057

$$\sum_{i=1}^{s-1}\frac{1}{x_i^{(j)}}+\frac{1}{x_s}+\frac{1}{x_{s+1}}-\frac{1}{x_1^{(j)}\cdots x_{s-1}^{(j)}x^s x_{s+1}}=1,$$

由于$\sum_{i=1}^{s-1}\frac{1}{x_1^{(j)}}+\frac{1}{x_1^{(j)}\cdots x_{s-1}^{(j)}}=1$，故上式给出

$$(x_s - n)(x_{s+1} - n) = n^2 - 1 = l_j(s),$$

这里$n = x_1^{(j)} \cdots x_{s-1}^{(j)}$。因为$l_j(s)$不是平方数，故$2 \mid d(l_j(s))$。$\frac{d(l_j(s))}{2}$对$l_j(s)$的因子$f_j$，$\frac{l_j(s)}{f_j}$给出方程(5)的$\frac{d(l_j(s))}{2}$个解，故总共给出方程(5)的$\sum_{j=1}^{\Omega(s-1)} \frac{d(l_j(s))}{2}$个解。因为当$u_1$，…，$u_s$是(3)的一组解，则$u_1$，…，$u_s$，$u_1 \cdots u_s - 1$是(5)的一组解，故$\Omega(s)$个(3)的解也可给出$\Omega(s)$个(5)的解(其中有$\Omega(s-1)$个且仅有$\Omega(s-1)$个解已在$\sum_{j=1}^{\Omega(s-1)} \frac{d(l_j(s))}{2}$中计算过）。于是

$$A(s+1) \geqslant \Omega(s) - \Omega(s-1) + \sum_{j=1}^{\Omega(s-1)} \frac{d(l_j(s))}{2}$$

$$= \Omega(s) + \sum_{j=1}^{\Omega(s-1)} \left(\frac{d(l_j(s))}{2} - 1 \right)。证毕。$$

因为$l_j(s) = (x_1^{(j)} \cdots x_{s-1}^{(j)})^2 - 1$在$s \geqslant 3$时是合数，故$d(l_j(s)) \geqslant 4$，因此由(4)给出：在$s \geqslant 3$时有

$$A(s+1) \geqslant \Omega(s) + \Omega(s-1)。$$

对$A(s)$，孙琦和曹珍富先后不断改进，有以下一系列结果：

定理3[25] 设$s \geqslant 9$，则$A(s+1) \geqslant \Omega(s) + \Omega(s-1) + 6$，且在$2 \mid s \geqslant 9$时$A(s+1) \geqslant \Omega(s) + \Omega(s-1) + 10$。

定理4[21] 设$s \geqslant 9$，则$A(s+1) \geqslant \Omega(s) + \Omega(s-1) + 10$，且在$2 \mid s \geqslant 12$时$A(s+1) \geqslant \Omega(s) + \Omega(s-1) + 14$。

定理5[22] 设$s \geqslant 10$，则$A(s+1) \geqslant \Omega(s) + \Omega(s-1) + 16$，且在$2 \mid s \geqslant 12$时$A(s+1) \geqslant \Omega(s) + \Omega(s-1) + 18$。

定理6[23] 设$s \geqslant 10$，则$A(s+1) \geqslant \Omega(s) + \Omega(s-1) +$

34，且在$2|s\geqslant 12$时$A(s+1)\geqslant \Omega(s)+\Omega(s-1)+46$。

我们[24]猜想：对$s\geqslant 3$有$A(s+1)>A(s)$。这个猜想在s不太大时已经得到证明，但对一般情形不易证明。另外，由$A(s)$与$\Omega(s)$的关系可知，如果我们定出了$A(s)$的主项，则$\Omega(s)$的主项也可能被定出。

§5 与单位分数相关的问题

现在我们利用前面关于单位分数的结果，来研究1972年Znám提出的一个问题。

［Znám问题］是否对每一个整数$s>1$，都存在整数$x_i>1(i=1,\cdots,s)$，使得对每一个i，x_i是$x_1\cdots x_{i-1}x_{i+1}\cdots x_s+1$的真因子？

这个问题与同余式组

$$x_1\cdots x_{i-1}x_{i+1}\cdots x_s+1\equiv 0(\mathrm{mod}\ x_i),x_i>1,i=1,\cdots,s;s>1 \tag{1}$$

有关。一个十分明显的结论是：如果设同余式组(1)的解满足$1<x_1<\cdots<x_s$，则在$x_s\neq x_1\cdots x_{s-1}+1$时，(1)的解便给出Znám问题的解。

1973年，Mordell[29]提出了求同余式组

$$x_1\cdots x_{i-1}x_{i+1}\cdots x_s\pm 1\equiv 0(\mathrm{mod}\ |x_i|),\ i=1,\cdots,s$$

的非零整数解的问题，并在$1\leqslant s\leqslant 5$时给出了部分解。1975年Skula[30]给出了同余式组(1)在$1<s\leqslant 4$时的全部解，从而证明：在$1<s\leqslant 4$时不存在Znám问题中要求的整数。

不失一般设适合Znám问题的整数x_1，…，x_s满足$1<x_1<\cdots<x_s$，则$(x_1,\ \cdots,x_s)$称为Znám问题的解。以$Z(s)$表示Znám问题的解的个数。1978年，Janák和Skula[19]证

明了$Z(5)=2$，$Z(6)=5$和$Z(7)\geqslant 10$。1983年，孙琦[31]彻底解决了Znám问题，他证明了

定理1 设$s\geqslant 5$,则$Z(s)\geqslant \Omega(s)-\Omega(s-1)>0$，这里$\Omega(s)$表方程

$$\sum_{i=1}^{s}\frac{1}{x_i}+\frac{1}{x_1\cdots x_s}=1,\quad 1<x_1<\cdots<x_s \tag{2}$$

的解的个数。

这个定理的证明是容易的，例如只要注意到方程(2)的$\Omega(s)$个解中恰有$\Omega(s-1)$个解是由$x_s=x_1\cdots x_{s-1}+1$产生的即可。

由这个定理，利用方程(2)的结果(§3)可得到下面一系列的结果：

Ⅰ.[18] 设$s\geqslant 5$，则$Z(s)>0$；

Ⅱ.[20] 设$s\geqslant 11$，则$Z(s)\geqslant 3$，且在$2\nmid s\geqslant 11$时$Z(s)\geqslant 5$；

Ⅲ.[21] 设$s\geqslant 11$,则$Z(s)\geqslant 5$,且在$2|s\geqslant 12$时$Z(s)\geqslant 7$；

Ⅳ.[22] 设$s\geqslant 12$,则$Z(s)\geqslant 8$,且在$2|s\geqslant 12$时$Z(s)\geqslant 9$；

Ⅴ.[23] 设$s\geqslant 12$,则$Z(s)\geqslant 17$,且在$2|s\geqslant 12$时$Z(s)\geqslant 23$。

1986年，孙琦和曹珍富[21]建立了Znám问题与同余式组(1)的一个等式，得到了如下的

定理2 设$s>2$，则$Z(s)=H(s)-H(s-1)$，这里$H(s)$表同余式组(1)的解$(x_1,\cdots,x_s)$$(1<x_1<\cdots<x_s)$的个数。

证 从(1)知$(x_i,x_j)=1(1\leqslant i\neq j\leqslant s)$，故(1)可化为

$$\sum_{i=1}^{s}x_1\cdots x_{i-1}x_{i+1}\cdots x_s+1\equiv 0(\mathrm{mod}\ x_i)\quad(i=1,\cdots,s),$$

此即

$$\sum_{i=1} x_1\cdots x_{i-1}x_{i+1}\cdots x_s+1\equiv 0(\bmod\ x_1\cdots x_s),$$

故可令

$$\sum_{i=1}^{s} x_1\cdots x_{i-1}x_{i+1}\cdots x_s+1=nx_1\cdots x_s,$$

这里n是正整数。由此得出

$$\sum_{i=1}^{s}\frac{1}{x_i}+\frac{1}{x_1\cdots x_s}=n,\ 1<x_1<\cdots<x_s, \qquad (3)$$

设$\Omega_n(s)$是方程(3)的解的个数，则有

$$H(s)=\sum_{n=1}^{\infty}\Omega_n(s),$$

且$\Omega_n(s)-\Omega_n(s-1)\geqslant 0$是在方程(3)的解中Znám问题的解的个数。故由$n\leqslant\frac{1}{2}+\cdots+\frac{1}{s}+\frac{1}{s!}$知

$$Z(s)=\sum_{n=1}^{\infty}(\Omega_n(s)-\Omega_n(s-1))=H(s)-H(s-1)。$$证毕。

由定理2可知，利用Ⅰ～Ⅴ的结果可以给出$H(s)$的一些估计，例如孙琦[32]证明了：如果$s\geqslant 4$，则$H(s)<H(s+1)$这方面最好的结果是[23]：如果$s\geqslant 11$，则

$$H(s+1)\geqslant H(s)+17$$

且如果$2\nmid s\geqslant 11$，则$H(s+1)\geqslant H(s)+23$。

参考文献

［1］ 柯召，孙琦，自然杂志，7（1979），411—413。

［2］ 柯召，孙琦，张先觉，四川大学学报（自然科学版），3（1964），23—37。

［3］ Yamamoto, K., Men. Fac. Sci. Kyushu University, Ser. A, 19（1965），37—47.

[4] Franceschine,N.,Egyptian Fractions,MA Dissertation,Sonoma State Coll.CA,1978.
[5] Rosati,L.A., Boll.Union Mat.Ital., (3) 9 (1954) ,59—63.
[6] Palamà,G.,Boll.Union Mat.Ital., (3) 13 (1958) ,65—72.
[7] Palamà,G.,ibid, (3) 14 (1959) ,82—94.
[8] Stewart,B.M.,Theory of Numbers,Macmillan,New York,1964,198—207.
[9] 刘元章，四川大学学报（自然科学版),2(1984),113—114。
[10] Vaughan,R.C.,Mathematika,17 (1970),193—198.
[11] Viola,C.,Acta Arith.,22 (1973),339—352。
[12] 单墫,数学年刊,7B (2) (1986) ,213—220。
[13] Mordell,L.J.,Canad.Math.Bull.,17(1974),149.
[14] 曹珍富，数学杂志,3 (1987) ,245—250。
[15] Guy,R.K.,Unsolved Problems in Number-Theory,D11,Springer—Verlag,1981.
[16] 冯克勤，魏权龄，刘木兰，科学通报,3(1987),164—168。
[17] 柯召，孙琦，四川大学学报(自然科学版),1 (1964) ,13—29。
[18] 孙琦,四川大学学报(自然科学版) ,2—3(1978),15—18。
[19] Janák,J.and Skula,L.,Math.Slovaca,28.

(1978) ,305—310.
[20] 孙琦，曹珍富，数学研究与评论,1 (1987) ,125—128。
[21] 孙琦,曹珍富,数学进展,3 (1986) ,329—330。
[22] 曹珍富,刘锐,张良瑞,J.Number Theory,27 (1987) ,206—211。
[23] 曹珍富,On the number of solution of the Diophantine equation $\sum_{i=1}^{s}\frac{1}{x_i}+\frac{1}{x_1\cdots x_s}=1$ 纪念华罗庚数论与分析国际学术会议（1988年8月,北京）上的报告论文。
[24] 曹珍富,河池师专学报,1 (1987) ,1—8。
[25] 孙琦，曹珍富，科学通报，2 (1985) ,155。
[26] Szabo,N.S.and Tanaka,R.I.,Residue Arithmetic and Its Applications to Computer Technology,McGraw—Hill,Inc.1967.
[27] 孙琦,曹珍富,自然杂志,9 (1985) ,669—670。
[28] 孙琦,数学研究与评论,4 (1986),149—154。
[29] Mordell,L.J.,Canad.Math.Bull.,16(1973), 457—462.
[30] Skula,L.,Acta Fac.Rer.natur.Univ.Comenianae,Mathematica,32 (1975) ,87—90.
[31] 孙琦,四川大学学报（自然科学版）,4 (1983), 9—11。
[32] 孙琦,科学通报,19 (1982) ,1159—1160。

方程类型索引

这表示求方程$x^2-Dy^2=k$与$y^2-D_1z^2=m$的公解。

三次方程

$x^3 \pm 1 = y^2$ 【209】

$x^3 - 1 = 2y^2$ 【21,210】

$x^3 + 1 = 2y^2$ 【25,113,210】

$x^3 - 1 = 7y^2$ 【113,210】

$x^3 - 1 = 23y^2$ 【210】

$x^3 - 1 = 3y^2$ 【245】

$x^3 \pm 1 = Dy^2$ 【26,210,211,225】

$x^3 + b = Dy^2, x^3 + b = 3Dy^2, b \in \{\pm 1, \pm 8\}$ 【209】

$x^3 \pm 8 = Dy^2, x^3 \pm 8 = 3Dy^2$ 【213-217】

$y^2 = x^3 + k(u^2 = v^3 - \eta)$ 【123,225,193】

$y^2 = x^3 + 7, y^2 = x^3 - 3$ 【17】

$y^2 + 28 = x^3, y^2 + 999 = x^3$ 【200】

$y^2 - kf^2 = x^3$ 【200】 $y^2 - Dm^2 = x^3$ 【94】

$u^2 = v^3 - \lambda v - \eta$ 【192】

$ey^2 = ax^3 + bx^2 + cx + d$ 【192】

$y(y+1) = x(x+1)(x+2), 2y^2 = x^3 - 4x + 2$ 【207】

$\frac{y(y+1)}{2} = \frac{x(x+1)(x+2)}{6}$ 【207】

$6y^2 = (x+1)(x^2 - x + 6)$ 【208】

$6y^2 = x(x+1)(2x+1)$ 【69,202】

$y^2 = 2ax^3 + (6 - 2a - 2c + 8b)x^2 + 2cx - d^2$ 【208】

$y^2 = (x-1)^3 + x^3 + (x+1)^3 = 3x(x^2+2)$ 【209】

$y^2 = 4cx^3 + 13(c = 1,3,9)$ 【217】

$x^2 + x + 1 = y^3, x^2 + x + 1 = 3y^3$ 【220】

$x^3 + dy^3 = 1$ 【105,219】

$x^3+8=Dy^3$ 【220】

$ax^3+by^3=c$ 【221】

$ax^3+by^3+cz^3=d$ 【237-238】

$x^3-my^3=nz^3, ax^3+by^3+cz^3=0$ 【240】

$x^3+dy^3=3z^3$ 【241】

$z^3=g(x,y)$ 【245】

$x^3+y^3=2z^3$ 【245】

$x^3+y^3+z^3=0$ 【33,103,233】

$x^3+y^3=pz^3$ 【98-99】

$x_1^3=2x_2^3+px_3^3$ 【15】

$x^3+y^3+2z^3=1$ 【97】

$x^3+y^3=2pz^3$ 【103】

$x^3+y^3+z^3=n$ 【232】

$x^3+y^3+z^3=1$ 【234】

$x^3+y^3+z^3=2$ 【102,234】

$x^3+y^3+z^3=3$ 【97,235】

$x^3+y^3+z^3=6, x^3+y^3+z^3=9$ 【103】

$x^3+y^3+z^3=30$ 【237】

$x^3+y^3+z^3=3a^3$ 【236】

$x^3+y^3+z^3=9a^3$ 【235】

$z^2=f(x,y)$ 【242】

$z^2=x^3+y^3, 2z^2=x^3+y^3, z^2=x^3+4y^3$ 【244】

$x^2+ky^2=z^3$ 【222-223】

$x_1^3+x_2^3+x_3^3=9x_4\pm 4$ 【11】

$x_1^3+2x_2^3+4x_3^3=9x_4^3$ 【12】

$x_1^3+3x_1^2x_2+x_2^3=9x_3\pm 2$ 【12】

$x_1^3+3x_1^2x_2+x_2^3=(9a+2)x_3^3$ 【12】

$x_1^3+2=7x_2, x_1^3+2x_2^3=7(x_2^3+2x_4^3)$ 【13】

$x_1^3+2x_2^3+4x_2^3+x_1x_2x_3=0$ 【17】

$x^3+3xy^2-3y^3=1$ 【108,218】

$x^3-3xy^2-3y^3=1$ 【109】

$x_3+ax^2y-(a+1)xy^2+y^3=1$ 【109】

$x^3+x^2y-2xy^2-x^3=1$ 【113,225】

$x^3-4xy^2+2y^3=1$ 【113,200,226】

$x^3-3xy^2+y^3=1$ 【225】

$x^3-12xy^2-12y^3=1$ 【226】

$a_1x^3+3a_2x^2y+3a_3xy^2+a_4y^3=a_5^3$ 【198】

$ax^3+by^3+cz^3-dxyz=0$ 【99,241】

$x^3+y^3+z^3=xyz, x^3+y^3+5z^3=5xyz$ 【241】

$ax^3+by^3+c=xyz$ 【245】

$x^2+y^2-x-y+1=xyz$ 【245】

$x^3+y+1=xyz$ 【245】

$x^3+y^2-y+1=xyz$ 【246】

$x^3+y^3+1=xyz$ 【247】

$x^3+y^3+z^3+w^3=n=0$ 【248】

$n\neq 0$ 【252】

$ax^3+by^3+cz^3+dw^3=n$ 【253】

四次方程

$1+x^2=2y^4$ 【4,62,289】

$x^4-2y^2=1$ 【19,27】

$x^2-8y^4=1$ 【25】

$x^2-2y^4=1$ 【26】

$x^2-27y^4=-2$ 【56,217】

$3x^4-2y^2=1$ 【69,261】

$(2y^2-3)^2=x^2(3x^2-2)$, $x^2-3y^4=1$ 【69】

$x^4-2y^4=1$ 【111】

$x^4-8y^4=1$ 【113】

$x^4-3y^2=-2$, $x^2-3y^4=-2$ 【217】

$x^2-5y^4=11, \pm 44$ 【294】

$x^2-2y^4=p$, $x^2-8y^4=p$ $(p=17,41,73,89,97)$ 【295】

$x^4-5y^2=11$, $x^4-5y^2=-44$ 【294】

$(x^2-2y^2)^2-2y^4=-1$ 【61】

$(2^e py^2-1)^2+1=2z^2$ 【69】

$x^4-py^2=1$ 【25】

$4x^4-py^2=1$ 【20】

$x^4-Dy^2=1$ 【49,64-65,260】

$x^2-Dy^4=1$ 【49,273】

$4x^4-Dy^2=-1$ 【48,283】

$4x^4-Dy^2=1$ 【271】

$x^2-4Dy^4=1$ 【275】

$x^2-5qy^4=1$ 【280】

$x^4-Dy^2=-1$, $x^2-Dy^4=-1$ 【287】

$4x^4-Dy^4=-1$ 【285】

$4x^4-pqy^4=-1$ 【280】

$x^4-Dy^4=\pm 1$ 【282,289】

$x^2\pm 4=Dy^4$ 【289,292-293】

$a^2x^4-Dy^2=\pm 1$ 【287,293】

$N^2x^4\pm 4=Dy^2$ 【293-294】

$x^2-Dy^4=k$, $x^4-Dy^2=k$ 【92,294-295】

$Ax^4 - By^2 = c(c=1,4)$ 【292】

$y^2 - 2c^2x^4 = p(c=1,2)$ 【295】

$(Mx^2 - N)^2 = My^2 - N, y^2 + (y+1)^2 = (x^2 + (x+1)^2)^2$ 【179】

$dy^2 = ax^4 + bx^2 + c$ 【290】

$x(x+1)(x+2)(x+3) = 2y(y+1)(y+2)(y+3)$ 【69,291】

$x(x+1)(x+2)(x+3) = 3y(y+1)(y+2)(y+3)$ 【61,291】

$y(y+1)(y+2)(y+3) = 5x(x+1)(x+2)(x+3)$ 【291】

$2y(y+1)(y+2)(y+3) = 3x(x+1)(x+2)(x+3)$ 【291】

$y(y+m)(y+2m)(y+3m) = 2x(x+m)(x+2m)(x+3m)$ 【292】

$y^2 + k^2 = (lx^2 - h)(rx^2 - s)$ 【290】

$y^2 + 1 = (4x^2 - 17)(8x^2 - 10), y^2 + 1 = (4x^2 - 17)(rx^2 - s)$ 【290】

$\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2}$ 【290】

$x^4 - 4x^2y^2 + y^4 = n$ 【297－298】

$x^4 + kx^2y^2 + y^4 = z^2$ 【29,298】

$k = \pm 1$ 【30－31】 ,$k = \pm 6$ 【29】 ,$k = 14$ 【33】

$ax^4 + bx^2y^2 + cy^4 = dz^2$ 【303】

$x^4 + y^4 = z^2$ 【26】

$x^4 - y^4 = z^2$ 【27】

$4x^4 + y^4 = z^2, x^4 + y^4 = 2z^2$ 【28】

$x^4 - y^4 = 2z^2$ 【33】

$x_1^4 = 2x_2^4 + px_3^4$ 【15】

$x_1^4 = px_2^4 + 2x_3^2$ 【17】

$x^4 + 2py^4 = z^2, x^4 = y^4 + pz^2$ 【33】

$ax^4 + by^4 = cz^2, x^4 + dy^4 = z^2$ 【303】

$(ax_1^2 + bx_2^2)^2 - 2k(cx_1^2 + dx_2^2)^2 = x_3^2$ 【17】

$x^4 + y^4 + z^4 = w^2$ 【23,304】

$ax^4 + by^4 + cz^4 = dw^4$ 【304】

$x^4 + y^4 + z^4 = w^4$ 【304】

$x^4 + y^4 = z^4 + w^4, x^4 + y^4 + 4z^4 = w^4$ 【305】

$x_1^4 + x_2^4 + x_3^4 + x_4^4 = x_5^4$ 【306－307】

高次方程（次数为n或＞4）

$x^2 - 1 = y^n$ 【18,45,51,71】

$1 + x^2 = y^n$ 【88,322】

$x^n - Dy^2 = 1$ 【94,329】

$x^q = y^p + 1$ 【70,123,126,329】

$x^n + 1 = y^{n+1},\quad x^2 = \dfrac{y^n + 1}{y + 1}$ 【80】

$x^p - y^p = D$ 【73】

$x^p + 1 = 2y^p$ 【45】

$x^6 - Dy^2 = 1$ 【55】

$x^2 + 2 = y^n$ 【94，321】

$x^{2n} - Dy^2 = 1$ 【312】

$x^p + 1 = 2y^2$ 【312】

$x^p - 1 = 2y^2$ 【55，312】

$x^{2n} - Dy^{2n} = 1$ 【315】

$x^{2n} - Dy^{2m} = 1$ 【316】

$x^2 - Dy^{2n} = 1$ 【316】

$1 + Dx^2 = 2y^n$, $1 + Dx^2 = 4y^n$ 【319】

$x^2 + D = y^n$ 【319】

$x^2 + p^2 = y^n$ 【320】

$x^2 + 2^m = y^n$ 【321】

$x^2 + 1 = 2y^n$, $2x^2 + 1 = y^n$ 【322】

$x^2 + 3 = y^n$, $x^2 + 5 = y^n$, $x^2 + 12 = y^z$, $x^2 + 28 = y^z$ 【323】

$x^2 + 8D = y^n$ 【322】

$x^2 + 4D = y^n$ 【323】

$cx^2 + D = y^n$ 【324】

$cx^2 + 4D = y^n$ 【324】

$3x^2 + 28 = y^n$ 【326】

$x^2 + D = 4y^n$ 【326】

$z^2 + z + 1 = y^n$, $z^2 + z + 1 = 3y^n$, $z^2 + z + \frac{D+1}{4} = y^n$ 【327】

$x^2 + 11 = 4y^n$ 【329】

$x^2 + 11 = 4y^5$ 【94】

$ax^2 + bx + c = dy^n$ 【319】

$ax^m - by^n = c$ 【329】

$ax^n - by^n = \pm 1$ 【331】

$ax^{2n} - by^{2n} = c$ 【332】

$ax^m + by^m = ax^n + by^n$ 【335】

$(x + y\sqrt{-1})^p + (x - y\sqrt{-1})^p = 2$ 【38】

$(x + y\sqrt{-2})^p + (x - y\sqrt{-2})^p = 2$ 【36】

$f(x, y)=g(x, y)$ 【117】

$\frac{x^m-1}{x-1}=y^n$ 【80, 129, 333】

$a\frac{x^n-1}{x-1}=y^m$ 【334】

$a\frac{x^m-1}{x-1}=b\frac{y^n-1}{y-1}$ 【335】

$f(x_1, \cdots, x_n)=0$ 【3, 16】

$xy=cz^l$ 【87】

$x^n+y^n=z^n$ 【2—4, 101, 129, 342】

$x^{2p}+y^{2p}=z^{2p}$ 【43, 348】

$x^{2p}+y^{2p}=z^2$, $x^{2p}-y^{2p}=z^2$, $x^{2p}+y^{2p}=z^p$,

$x^{2p}-y^{2p}=z^p$ 【348】

$x^p-y^p=Dz^2$ 【43】

$\frac{x^p-y^p}{x-y}=p^2z$ 【34】

$y^2=p\frac{x_1{}^p-x_2{}^p}{x_1-x_2}$ 【41】

$y^m=x(x+1)\cdots(x+n-1)$ 【338】

$\sum_{j=0}^{h}(x-j)^n=\sum_{j=1}^{h}(x+j)^n$ 【337】

$\sum_{j=0}^{h}(x+j)^n=(x+h+1)^n$ 【339】

$\sum_{j=0}^{n-1}(x+jr)^t=(x+nr)^t$ 【340】

$\sum_{j=1}^{m-1}j^n=m^n$ 【340】

指数方程

$2^x-3^y=1$ 【38】

$(4n^2-1)^x+(4n)^y=(4n^2+1)^z$ 【364】

$1+p^a=q^b r^c+p^d q^e r^f$ 【367】

$(p, q, r)=(2,3,5), (3,2,5), (5,2,3)$ 【368】

$1+p^a=q^b 2^c+p^d q^e 2^f$ 【370】

$1+p^a=q^b+p^d$ 【370】

$1+y=z$, $yz=2^a 3^b 5^c 7^d$ 【370】

$x+y=z$, $xyz=2^a 3^b 5^c 7^d$ 【370】

$1+2^a+7^b=3^c+5^d$, $3^a+7^b=3^c+5^d+2$, $3^a+5^b+7^c=11^d$ 【371】

$a^x-b^y c^z=\pm 1, \pm 2$ 【371】

$x^2=4q^m+4q^2+1$ 【123, 387】

$x^2=4q^{a/2}+4q+1$ 【386】

$x^2=4q^m+4q+1$ 【387】

$x^2=4q^n-4q+1$ 【389】

$x^y y^x=z^z$, $x^y y^z=z^x$, $x^x y^z=z^y$ 【385】

$x^x y^y=z^z$ 【4, 75, 378】

$\prod_{i=1}^{k} x_i^{x_i}=z^z$ 【76, 379】

$\alpha^n+\beta^n=2x^2$, $\alpha^{4m}+\beta^{4m}=2x^2$ 【389】

$\alpha^{2m}+\beta^{2m}=2x^2$ 【390, 55】

其它类型的方程

$\binom{n}{m}=y^k$ 【5】

$n!+1=x^2$, $n!=x^p\pm y^p$ 【5】

$\binom{n}{2}=y^k$ 【45, 317】

$x^{\frac{1}{m}}+y^{\frac{1}{n}}=z^{\frac{1}{r}}$ 【74】

$x^{\frac{m_1}{n_1}} + y^{\frac{m_2}{n_2}} = z^{\frac{m_3}{n_3}}$ 【75】

$\frac{\omega^x - \overline{\omega}^x}{\omega - \omega} = -1$ 【110】

$\sum_{i=1}^{n} \delta_i x_i = 0, \ \delta_i \in \{-1, 1\} \ (i = 1, \cdots, n)$ 【367】

$1 + \delta_1 \backslash (1) + \delta_2 \Gamma(1) + \delta' \chi^{(m)}(1) = 0$ 【368】

$N(x_1\omega_1 + \cdots + x_n\omega_n) = a$ 【103】

$a + bn + cn = 4abcd, \ na + b + c = 4abcd$ 【421】

$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ 【124, 400】

$\frac{4}{p} = \frac{1}{px} + \frac{1}{y} + \frac{1}{z}, \ \frac{4}{p} = \frac{1}{x} + \frac{1}{py} + \frac{1}{pz}$ 【402】

$\frac{5}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ 【403】

$\frac{5}{121} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ 【403】

$\frac{m}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ 【400】

$\sum_{i=0}^{k} \frac{1}{x_i} = \frac{a}{n}$ 【126, 404】

$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w} + \frac{1}{xyzw} = 0$ 【77, 404】

$\frac{1}{x} = \frac{1}{y} + \frac{1}{z} + \frac{1}{w} + \frac{1}{xyzw}$ 【78, 404】

$\frac{1}{x} + \frac{1}{y} + \frac{1}{xyzw} = \frac{1}{z} + \frac{1}{w}$ 【78, 404】

$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{1}{w}+\frac{1}{xyzw}$ 【78, 404】

$\frac{1}{x}=\frac{1}{y}+\frac{1}{z}+\frac{1}{xyz}$ 【406, 411】

$\frac{1}{x_1}=\frac{1}{x_2}+\cdots+\frac{1}{x_s}+\frac{1}{x_1\cdots x_s}$ 【80, 407—408】

$\frac{1}{x_1}+\cdots+\frac{1}{x_k}=1$ 【409】

$\frac{1}{x_1}+\cdots+\frac{1}{x_s}+\frac{1}{x_1\cdots x_s}=1$ 【79, 410—411, 418, 422】

$\sum_{i=1}^{s}\frac{1}{x_i}-\frac{1}{x_1\cdots x_s}=1$ 【417—418】

$\sum_{i=1}^{s}\frac{1}{x_i}+\frac{1}{x_1\cdots x_s}=n$ 【423】

人 名 索 引

A

B

C

D

E

F

G

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

[General Information]
书名=丢番图方程引论
作者=曹珍富著
页数=451
SS号=10831576
DX号=
出版日期=1989年03月第1版
出版社=哈尔滨工业大学出版社